

G-Cloud 10 Call-Off Contract

This Call-Off Contract for the G-Cloud 10 Framework Agreement (RM1557.10) includes:

Part A - Order Form 2

Schedule 1 - Services 51

Schedule 2 - Call-Off Contract charges 5451

Part B - Terms and conditions 5452

Schedule 3 - Collaboration agreement 7471

Schedule 4 - Alternative clauses 7471

Schedule 5 - Guarantee 7571

Schedule 6 - Glossary and interpretations 7572

Schedule 7 - Processing, Personal Data and Data Subjects 8682

# Part A - Order Form

|  |  |
| --- | --- |
| **Digital Marketplace service ID number:**  | 322803416669880  |
| **Call-Off Contract reference:**  |   |
| **Call-Off Contract title:**  | Wintel Transition & Support Service  |
| **Call-Off Contract description:**  | Provision Wintel Support within EUC Services for Highways England  |
| **Start date:**  | 5th November 2018  |
| **Expiry date:**  | 24 months from start date  |
| **Call-Off Contract value:**  | **Wintel Service** Year 1: £79,640 per month Year 2: £53,093 per month Total: £1,592,796  |
| **Charging method:**  | Fixed Service Price  |
| **Purchase order number:**  | To be advised by the buyer  |

This Order Form is issued under the G-Cloud 10 Framework Agreement (RM1557.10).

Buyers can use this order form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Deliverables offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

|  |  |
| --- | --- |
| **From: The Buyer**  | *Redacted*Highways England Company Limited  Buyer’s main address: Bridge House 1 Walnut Tree Close Guildford  |
|  | Surrey GU1 4LZ  |
| **To: The Supplier**  | *Redacted*Netcompany UK Limited Supplier’s address: 46-54 High Street Ingatestone Essex CM4 9DW Company number: 08568559  |
| **Together: the ‘Parties’**  |

# Principle contact details

|  |  |
| --- | --- |
| **For the Buyer:**  | Name: *Redacted* Email: *Redacted*Phone: *Redacted*  |
| **For the Supplier:**  | Title: *Redacted*Name: *Redacted* Email: *Redacted* Phone: *Redacted*  |

# Call-Off Contract term

|  |  |
| --- | --- |
| **Start date:**   | This Call-Off Contract Starts on 05/11/18 and is valid for 24 months  |
| **Ending** **(termination):**  | The notice period needed for Ending the Call-Off Contract is at least 90 Working Days from the date of written notice for disputed sums or at least 30 days from the date of written notice for Ending without cause.  |
| **Extension period:**  | This Call-Off Contract can be extended by the Buyer for 2 period(s) of 12 months each, by giving the Supplier 3 months written notice before its expiry and capability to align the extended pricing adjusted for inflation.  |
|  | Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.  |

# Buyer contractual details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

|  |  |
| --- | --- |
| **G-Cloud Lot:**  | This Call-Off Contract is for the provision of Services under: Lot 3 - Cloud support  |
| **G-Cloud services required:**  | The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:  In summary, the Supplier shall provide build, management and remote support (2nd and 3rd line) of the Highways England End User Compute estate. This includes all Windows based PCs on the estate that are using Windows 7, Windows 8.1 and Windows 10, SurfaceHubs and the supporting infrastructure services including AD, SCCM and SCOM where relevant to the delivery of the EUC Wintel Services.  The high-level requirements include, but are not limited to, the following aspects:  * Manage all the end user devices (PCs, Laptops, Windows tablets, SurfaceHubs).
* Create, support and manage the ongoing development of the Windows operating system build for Highways England, updating the existing document set to reflect the changes.
* Obtain the relevant patches from Microsoft and deploy the patches and upgrades as required and through the required change control processes to the end user devices. Patches should be rolled up and deployed under the monthly patching cycles.
* Provide application packaging services to package applications that are required for automated deployment through the SCCM infrastructure to the end user devices and commence preparatory works for the introduction of Microsoft Store for the Customers End Users as soon as practicably possible and agreed with the Customer.
* Support Daisy in their 1st line activities to support the management of user accounts and relevant accessibility to the tools required to support their activities.
 |

|  |  |
| --- | --- |
|  | * Provide 2nd and 3rd line remote support for the end user compute estate and supporting technologies
* Work collaboratively with the other Highways England tower Suppliers in support of the end to end service
* Manage the deployment and support of standard desktop applications including Microsoft Office desktop (including Outlook mail) and Office 365 components, Web browsing software (both IE11 and Chrome).
* Manage and support the core infrastructure services that underpins the end user compute devices including Active Directory, Microsoft Exchange, SCCM, SCOM, McAfee AV, InTune, Azure AD and Azure common components.
* Work with Highways England Service Management, Service Design and Security to ensure Service improvements are identified and brought to the relevant governance boards for review and approval.
* Transition the service to Highways England internal resources at the end of the contract, providing the required shadowing and reverse shadowing and current documentation to enable a smooth transition.

 The commencement of Service shall be on 17th December 2018 from the current incumbent Supplier, CGI, with knowledge transfer and shadowing activities happening before the commencement date and following a go-live decision from Highways England.  The following detailed requirements shall be delivered by the Supplier in delivering the Wintel Transition & Support Service for Highways England.  1. **Installation, Moves, Adds, Changes and Disposals (IMACD)**
	1. The WinTel Supplier shall work with the Customers’ Desk Side

Support provider, and where appropriate, the HELITS (Highways England Local IT Support) team in relation to on-site desk-side services, where required to deliver the services specified. * 1. The WinTel Supplier shall implement major changes with minimum disturbance to Users. If on-site activity on the End User Device is required, in conjunction with the Customers’ Deskside Support Supplier and the HELITS team, this should, where appropriate, be planned to occur outside normal business hours (07:00-19:00 Monday to Friday) for office based users or as otherwise agreed between the Customer and the WinTel Supplier. For operational users it shall be with agreement from the Customer.
 |

|  |  |  |
| --- | --- | --- |
|  |  | 1.3 The WinTel Supplier shall minimise, and where possible avoid, the need for inter-operation between different build versions where a number of different build (image) versions exist across the estate.  |
|  |  **2.**  | **Support Services** 2.1 The WinTel Supplier shall provide remote 2nd and 3rd line support to all User Groups in accordance with their support needs across the Highways England office locations. Homeworkers should be supported as if they are on a Main Site.  2.2 The WinTel Supplier shall provide the stated service: 2.2.1 07:00 – 19:00 Monday to Sunday including bank holidays for the Main Sites; 2.2.2 Twenty four (24) hours seven (7) days a week including bank holidays for the RCCs, the Outstations and NTOC (as per the site list issued by the Customer, inclusive of the ability to include 20% growth of the estate through the terms of the contract), provided by on call resources out of core hours; 2.2.3 Twenty four (24) hours seven (7) days a week including bank holidays for Email Availability Support for all Users provided by on call resources out of core hours; 2.2.4 Twenty four (24) hours seven (7) days a week including bank holidays for the site hosting ‘Gold Command’ for the required duration, reverting back to standard site hours as defined below once ‘Gold’ Command’ is removed. Note that 'Gold Command' was last invoked by Highways England in 2012. 2.3 The WinTel Supplier shall comply with the Customer’s office security requirements and physical access arrangements and the HMG Security Policy Framework for access to any Customer Premises including Home Workers. 2.4 The WinTel Supplier shall provide advice and guidance on the operability and inter-operability of Hardware and Software, where relevant to the EUC Wintel services. 2.5 The WinTel Supplier shall advise the Customer of any developments in best practice, research findings, and User guidance in respect of its obligations under this Agreement and in relation to the Management of Health and Safety at Work (Amendment) Regulations 2006 for IT and voice telephony services as soon as it becomes aware of any change.  |

|  |  |  |
| --- | --- | --- |
|  |   | 2.6 The WinTel Supplier shall assist the Customer in promulgating advice approved by the Customer to Users via appropriate channels (normally corporate email). 2.7 The WinTel Supplier shall co-operate with any third party employed by the Customer to carry out electrical testing of portable IT equipment which shall include any equipment provided or supported by the WinTel Supplier.  |
|  | **3.**   | **Device Repair and Maintenance** 3.1 The WinTel Supplier shall schedule preventive maintenance to EUC Assets outside of normal business hours (07:00-19:00) and only within agreed maintenance windows, except in exceptional circumstances and with the agreement of the Customer. 3.2 The WinTel Supplier shall comply with the Customers or 3rd Party Code of Connections should it wish to make connection to the Customer’s network for any reason.  |
|  | **4.**  | **Software Build Management**  4.1 The Customer provides a Windows 7 End User Device build for the majority of Users, and a Windows 8.1 build for some Tablet users. The Customer is currently involved in a Modernising Workplace project that will provide a Windows 10 desktop build for almost all users, on a one device per user basis, including Office 365, This project is currently scheduled to complete by the March 2019. The WinTel Supplier will be responsible for the ongoing maintenance and development of all builds, once they are part of Business as Usual following the completion of the migration project and once suitable handover has been provided from the Migration Supplier including a review of the proposed build, relevant documentation and workshops. 4.2 The WinTel Supplier shall provide a Software Build Management Service that develops, maintains, administers and supports the Customers’ Standard Builds for End User Devices. 4.3 The WinTel Supplier shall install the appropriate Standard Build on new or returned End User Devices or where required to resolve an Incident e.g. to recover from a catastrophic failure. 4.4 In providing the Software Build Management Service, the WinTel Supplier shall: 4.4.1 support, develop and maintain as few as possible Standard Builds for End User Devices;  |

|  |  |
| --- | --- |
|  | 4.4.2 maintain and support all End User Devices regardless of whether they utilise a Standard Build or Non-Standard Build; 4.4.3 maintain and version control the Standard Builds by: 4.4.4 providing update releases of each Standard Build including updates such as Operating System service packs, device driver updates and other changes; 4.4.5 managing the upgrade of Standard Builds; 4.4.6 managing Standard Build version information on End User Devices; 4.4.7 test and incorporate any required manufacturer updates into the Standard Build; 4.4.8 distribute the Standard Build for End User Devices, in conjunction with the Customer and other Suppliers; 4.4.9 evaluate the impact of new software, operating system and security patches against the Standard Build; 4.4.10 document the Standard Build and making that documentation available to the Supplier’s builders and the Customer; 4.4.11 work with other IT Suppliers to ensure policy settings of the End User Devices are managed in accordance with the Customer’s policies; 4.4.12 manage and deliver the end-point configuration during the device lifecycle; 4.4.13 deliver the build and configuration in a secure and repeatable manner to a device; 4.4.14 provide reporting regarding the integrity of build and configuration deployed when the build is updated with a major update; 4.4.15 provide reporting regarding breaches or exceptions to the standard configuration or that deviate from the Customer’s policies; 4.4.16 restrict the ability to execute non-approved software on End User Devices and agree exceptions with the Customer through the allocation of elevated rights to individuals or groups; 4.4.17 provide restricted access for End Users to reduce the ability of End Users to make changes; 4.4.18 work with Highways England and their Suppliers to remove unrequired or inappropriate administration accounts to prevent access to the Internet, email etc for  |

|  |  |  |
| --- | --- | --- |
|  |   | Administrator accounts to restrict the vectors for malware infection.  |
|  | **5.**  | **Software Distribution** 5.1 The WinTel Supplier shall provide a Software Distribution Service that distributes and maintains an approved software catalogue to End User Devices in accordance with the Customer’s policies and the Service Levels.5.2 Highways England shall be responsible for all hardware and software procurements that is required to deliver the software to the end user devices. 5.3 In providing the Software Distribution Service, the WinTel Supplier shall: 5.3.1 manage the release of Software to the EUC device in accordance with the Customer’s Release Management process; 5.3.2 maintain and update the CMDB following Software Distribution in accordance with the Customer’s Change Management and Configuration Management processes; 5.3.3 distribute the following types of Software (providing compatibility with the build): * Software applications, working with other IT Suppliers as appropriate;
* version updates, fixes and patches to relevant Software, working with other IT Suppliers as appropriate;  anti-virus signatures to End User Devices.

5.3.4 for End User Devices that were not connected to the Customer’s network when Software was distributed, the End User Device shall commence receiving the relevant Software within one hour of being re-connected to the Customer’s network; 5.3.5 enable multiple software distribution options including deferred, staged or incremental, timed and immediate install; 5.3.6 upgrade End User Device Software (that is included in the approved software catalogue) when a new release is available as soon as is practical after the software distribution package passes the relevant acceptance criteria;  |

|  |  |  |
| --- | --- | --- |
|  |  | 5.3.7 maintain details of all approved Software that can be installed on End User Devices available via the Service Catalogue. 5.4 The WinTel Supplier shall manage the Software Distribution Service on behalf of other Suppliers to distribute any Software or Applications necessary to deliver the IT Services. 5.5 The WinTel Supplier shall work with other IT Suppliers to facilitate the distribution of software. 5.6 In providing the Software Distribution Service, the WinTel Supplier shall ensure that: 5.6.1 Applications can be installed silently with no User intervention (unless otherwise agreed with the Customer and pending application compatibility for silent installs); 5.6.2 Where practical, existing Applications are unaffected when new applications are installed. 5.7 Operating System or other Applications (both functional and non-functional characteristics) are not adversely affected when Applications are uninstalled. 5.8 The WinTel Supplier shall initiate regression plans to roll back any changes e.g. Service pack distribution and operating system upgrades, if deemed necessary by the Customer. 5.9 The WinTel Supplier shall lead the implementation of InTune, a product that the Customers intends to use as its primary Distribution Tool for all (including any introduction of Configurable Items), Windows devices including laptops, mobile devices, tablets and SurfaceHubs.  |
|  |  **6.**  | **Application Packaging** 6.1 The WinTel Supplier shall provide an Application Packaging Service that creates and maintains Application packages for the distribution of Software to End User Devices to allow Users to access the appropriate Applications from their End User Devices and to allow an Applications Maintenance Supplier or Other IT Supplier to fulfil their obligations. 6.2 The WinTel Supplier shall enable all Users to access all Applications for which they are authorised from all approved End User Devices while connected to the Customer’s network. 6.3 In providing the Application Packaging Service, the WinTel Supplier shall:  |

|  |  |
| --- | --- |
|  | 6.3.1 make details of all approved Application packages that can be installed on End User Devices available via the Service Catalogue; 6.3.2 work with Highways England to enable their users to perform functional regression testing of new or updated Application Packages between Standard Builds, and existing Application store and manage Application Packages and associated source code within the required storage location; 6.3.3 provide documentation for each Application Package where applicable to describe the installation method; 6.3.4 work with the Customer to rate applications as Simple, Medium, Complex to support the Impact Assessment of activities to complete the packaging process and where each application that is to be packaged will be jointly graded based upon what is known or expected of the Application. The following definitions apply. 6.3.5 **Grading Rules** – the rules and definitions which determine which process an Application will go through in the packaging stage, as well as the price per unit for that Application. 6.3.6 **Simple Application Package** means a package created for an Application which is installed on the Client only with no external system access requirements or software dependencies. Simple applications would include URLs which don’t link to any other application. Examples of simple applications are Notepad ++ and 7-Zip. 6.3.7 **Medium Application Package** refers to a package created to package an Application such as: * Any Application which is installed only on the client (has no external system access requirements) but which does require pre-requisite client software dependencies. java for installation;
* Any Client or Web Application with system access control requirements. e.g. Application requires Java / Active X installations to be linked;
* Any Web Application requiring reach-back to an internally and externally hosted web server;
* Any Applications that require additional components after installation (e.g. copying files, Reg Keys, Scripts);
 |

|  |  |  |
| --- | --- | --- |
|  |  | * Examples of medium complexity applications – Java, Chrome, Firefox.

6.3.8 **Complex Application Package** means a software package created to package: * Any client Application which requires connectivity to external systems such as Application server and / or internet / intranet integrations and may additionally have software dependencies;
* Any Application which requires sub-component Applications whereby the sub-components themselves have no other function except to enable the Application’s core function. – in such instances, the requisite subcomponents to form a functional Application unit will be managed as one Complex Application Package (although may be comprised of multiple packages);
* Any Application with multiple configurations per country requiring detailed configuration;
* Examples of complex applications – AutoCAD, Dragon Naturally Speaking, Zoomtext.
	1. Based on whether an application is Simple, Medium or Complex, The Supplier shall work with Highways England to determine the appropriate impact of each category to enable the implementation of templated impacts.
	2. Applications that fail the packaging and testing process shall be placed into remediation and the WinTel Supplier shall work with Highways England to determine and propose solutions to rectify the issues. These may require new application versions to be packaged or a separate project initiated to find an alternative method to deploy the application. The Supplier shall work with Highways England to agree when an application is required to enter into a Remediation status. The Supplier shall impact assess the additional effort required to deliver the solution to the EUC estate.
	3. The WinTel Supplier will provide the ability to utilise the

Customers own Microsoft Store and the ability to deploy using InTune for all Windows and mobile devices.  |
|  | **7.**  | **Testing and Validation** 7.1 The WinTel Supplier shall provide a Testing and Validation Service ensuring that all upgrades, releases and patches are tested in agreement with the Customer prior to release.  |

|  |  |  |
| --- | --- | --- |
|  | 7.2  | In providing the Testing and Validation Service the WinTel Supplier shall require: 7.2.1 Highways England to provide a small pool of End User Devices that the Supplier shall use to support each of the Standard Builds; 7.2.2 access to development and test environments defined by Highways England and relevant to the delivery of the EUC Wintel Service; 7.2.3 administration rights of development and test environments relevant to the EUC Wintel service.  |
|  | 7.3  | The WinTel Supplier shall provide a Testing Service to support testing for: 7.3.1 new End User Devices; 7.3.2 Active Directory; 7.3.3 Application Packaging in terms of successful application loading, functional testing and User Acceptance Testing (UAT) of the applications shall be completed by Highways England; 7.3.4 Build Management; 7.3.5 Software Distribution; 7.3.6 testing new Standard Builds.  |
|  | 7.4  | The WinTel Supplier shall ensure that Application Packages and Standard Builds are tested and within reason the application will load and not cause the other core applications to fail  |
|  | 7.5  | In providing the Testing Service, the WinTel Supplier shall: 7.5.1 provide security testing of End User Devices to ensure compliance with the Customer’s policies; 7.5.2 provide the following testing within agreed testing windows:  control testing;  vulnerability testing;  risk identification. 7.5.3 conduct quarterly scheduled or ad-hoc on-request vulnerability testing; 7.5.4 conduct tests in accordance with the Customer’s policies and report the results to the Customer; 7.5.5 review the results of testing and provide summary information to the Customer on identified vulnerabilities and appropriate corrective actions.  |

|  |  |  |
| --- | --- | --- |
|  | 7.6  | The WinTel Supplier shall co-operate with any organisation appointed by the Customer to independently assess its security provisions.  |
|  | 7.7  | The WinTel Supplier shall provide a Vulnerability Management Service to provide information on vulnerabilities identified on the estate or active in the wild and manage these through to remediation.  |
|  | 7.8  | In providing the Vulnerability Management Service, the WinTel Supplier shall: 7.8.1 manage the vulnerability processes, testing schedules, results and remediation; 7.8.2 enable a process to immediately patch or pull vulnerable services which have a high probability of being under immediate attack; 7.8.3 identify vulnerabilities through information provided by software vendors, industry bodies or the security community as well as through scheduled and ad-hoc testing; 7.8.4 operate the service, managing vulnerabilities in a structured and auditable way to remediation; 7.8.5 document vulnerability management policies and processes to include activities such as Patch Management, changing configuration or recommending changes in process, policy or behaviour as necessary to remediate the vulnerabilities; 7.8.6 provide regular and ad hoc reporting of vulnerability information including but not limited to systems at risk, remediation actions, patches applied, configurations changed; 7.8.7 monitoring the availability of anti-virus software updates, anti-virus signature updates and security releases relevant to the Services which are made generally available in the market and inform the Customer of any such update; 7.8.8 install all anti-virus software updates, anti-virus signature updates and security releases applicable to the Services; 7.8.9 monitor and manage the installation of patches appropriate to the operating systems and database software installed on End User Devices.  |
|  | 7.9  | In providing the Patching Service, the WinTel Supplier shall:  |

|  |  |  |
| --- | --- | --- |
|  |   | 7.9.1 test patches and hot fixes, where possible and relevant, for applications and operating systems, prior to incorporating them on the Standard Builds and Inherited Builds and distributing to the estate in accordance with the Customer’s policies; 7.9.2 in the event of any failed test, the WinTel Supplier shall: * produce a failure report highlighting the scope of the failure; the tests which were performed; and identification of those tests which failed;
* provide a recommendation on the different courses of action which are available to resolve the issue and risks associated with each course.
	1. The WinTel Supplier shall provide real time reporting of systems with vulnerabilities e.g. unpatched EUC devices or with weak configurations that have yet to receive the updates through the use of the systems that are available.
	2. If the systems inherited by the WinTel Supplier from the current incumbent Supplier are unable to deliver the required functionality, The WinTel Supplier shall work with Highways England to scope and specify the required systems and provide an appropriate impact assessment for the design and implementation of the system to deliver the required functionality.
	3. The WinTel Supplier shall implement security patches in line with the Release and Deployment Processes and Procedures contained in the Service Operations Manual.
	4. The WinTel Supplier shall ensure Security and antivirus updates are maintained at latest levels within ten (10) days of their release from the vendor, so that security vulnerabilities are minimised on both the client and the local server.
 |
|  | **8.**  | **Power Management: Environmental Impact** 8.1 The WinTel Supplier shall work with the Customer to ensure that End User Device builds are configured to best practice for energy management.  |
|  |  **9.**  | **Lifecycle Management** 9.1 The WinTel Supplier shall work with the IT Suppliers to manage the obsolescence of EUC Assets, Hardware and Software in accordance with National Cyber Security Centre requirements,  |

|  |  |  |
| --- | --- | --- |
|  |   | with the Customer’s policies and via consultation with the Customer. 9.2 The WinTel Supplier shall ensure that where it is viable/practicable, appropriate EUC Assets remain installed in the appropriate location for the appropriate lifespan to deliver maximum value for money.  9.3 The WinTel Supplier shall proactively identify inactive EUC Assets and coordinate the removal or reallocation of such EUC Assets with the guidance of the Highways England IT security team.  |
|  | **10.**   | **Application Performance Monitoring Service** 10.1 The WinTel Supplier shall collaborate with the Service Management Supplier and other IT Suppliers to support the base lining and subsequent performance monitoring of any new or changed Applications. 10.2 The WinTel Supplier shall provide a Capacity and Availability reporting service as agreed with the Customers' Service Management team (or equivalent Supplier)  |
|  | **11.**  | **Standalone (Internet and Bespoke) Devices** 11.1 The WinTel Supplier shall provide a standalone solution in Customer Premises in conjunction with the local HELITS team to allow Users to: 11.1.1 browse the internet independently outside of the Highways England IT network; 11.1.2 perform anti-virus checks on removable media; 11.1.3 Highways England shall provide the hardware and software required to deliver the Standalone devices.  |
|  |  **12.**  | **Inventory Management** 12.1 The WinTel Supplier shall provide an Inventory Management Service to manage the EUC Assets that are not deployed to Users or Customer Premises. 12.2 In providing the Inventory Management Service the WinTel Supplier shall: 12.2.1 define, maintain and agree with the Customer the specifications for EUC Assets and Standard Builds in line with the Customer’s policies; 12.2.2 agree with the Customer the technical requirements for EUC Asset procurement (including exceptions and  |

|  |  |  |
| --- | --- | --- |
|  |  | variants), including End User Devices, EUC Infrastructure and EUC Peripheral Devices; 12.2.3 define, maintain and agree with the Customer the forward schedule of EUC Assets to be procured by the Customer so as to achieve the Service Levels whilst minimising the Customer’s expenditure; 12.2.4 support the maintenance of a CMBD on behalf of the customer and in accordance with the Service Management function and keep the Customer’s CMDB updated with timely and accurate information on EUC Assets.  |
|  | **13.**   | **Hardware Support and Maintenance** 13.1 The WinTel Supplier shall provide a fully managed service for software resident on the local branch cache servers, working with the Desk Side Support provider as necessary. Where needed to meet resilience requirements or in response to the Customer’s data handling policy, local servers should replicate in accordance with industry practice with centrally hosted storage provided by the Hosting Supplier.  |
|  | **14.**  | **Access Control (Active Directory)** 14.1 The WinTel Supplier shall manage and secure each User’s access to the facilities they are entitled to use via the EUC Service through the use of authentication and authorisation services based on an appropriate, industry standards-based directory system. The WinTel Supplier shall utilise the existing Active Directory service that has been deployed to deliver the requirements. 14.2 In providing the Access Control Service the WinTel Supplier shall: 14.2.1 enable ‘single sign-on’ access to applications and rolebased access control (RBAC) as appropriate and supported by the application; 14.2.2 record, log and report key events within a schedule to be agreed with the Customer; 14.2.3 review the current and future provision of User profiles and categories and recommend improvement actions; 14.2.4 provide access to all IT Services and Applications where appropriate;  |

|  |  |  |
| --- | --- | --- |
|  |  | 14.2.5 manage and monitor the use and control of privileges and privileged accounts across the EUC Services; 14.2.6 enable the Customer Representative to request, provision, manage and revoke privileged User and system accounts and the associated credentials; 14.2.7 manage User’s accounts such that they have only the privileges necessary to perform their function; 14.2.8 manage and report on breaches of privileges where tools currently exist to provide this, attempts to subvert privileges or unauthorised attempts at accessing accounts; 14.2.9 report on privileged account creation, removal and account history; 14.2.10ensure that User’s ability to execute unauthorised programs from End User Devices is prohibited by restricting the ability to use removable media and ports such as, but not limited to, USB, Firewire, eSATA, and Thunderbolt on the current Windows 7 and 8.1 estate and work with Highways England Security to implement on the Windows 10 estate; 14.2.11The WinTel Supplier shall work with Highways England Security to design and implement the required functionality on the Windows 10 build where it currently does not align to the requirements or match that provided by the current Windows 7 build. Where new software may be required, Highways England shall procure for the Supplier to implement.  |
|  | 14.3  | Provide an automated facility to securely reset User passwords at account or Application level to the Service Management and IT Suppliers. (Note that these services are currently delivered using Microsoft services, and the Customer intends for this to continue.)  |
|  | 14.4  | The WinTel Supplier shall provide a self-service password reset capability. The self-service password reset capability shall uniquely identify the User with an authentication mechanism prior to permitting password reset.  |
|  | 14.5  | The WinTel Supplier shall monitor and report on password use for suspicious activity such as multiple password attempts or unusual password reset activity.  |

|  |  |
| --- | --- |
|  | 14.6 The WinTel Supplier shall ensure that Users have appropriate access rights to enable them to update their own personal details, and only their own details 14.7 The WinTel Supplier shall allow the Service Desk to add, delete or change User accounts in accordance with Service Requests received from the Customer. 14.8 The WinTel Supplier shall maintain User access profiles, including routine changes to User details and access rights in accordance with Service Requests received from the Customer or the Service Management Supplier. 14.9 The WinTel Supplier shall allow Users to request and make changes to their own User accounts including access to Application access, with appropriate authorisation or approval checks. 14.10 The WinTel Supplier shall ensure that only Users authorised by the Customer are able to access the IT Services. 14.11 The WinTel Supplier shall provide support to deploy a Single Sign-On (SSO) and Metadirectory services that shall manage the Single Sign-On and Metadirectory services and provide access to the service on request from other IT Suppliers for external (approved) applications where the applications are compatible with SSO functionality 14.12 In providing the SSO Service the WinTel Supplier shall: 14.12.1manage and support the SSO service components on End User Devices; 14.12.2manage and support the central directory service that stores encrypted User identity data such as usernames and passwords; 14.12.3manage and support the scripts that enter credentials on the End User Devices when a User attempts to access an Application; and 1. 12.4manage and support the centralised and distributed infrastructure used to provide the SSO Service.

14.13 The WinTel Supplier shall provide the tools and/or processes to enable the Service Management Supplier to undertake: 14.13.1User access control changes; 14.13.2remote control of End User Devices for support purposes; 14.13.3remote installation and/or removal of Software and Applications; 14.13.4Password resets.  |

|  |  |  |
| --- | --- | --- |
|  |   | 14.14 Where additional tools may be required within the current estate to support and deliver the above requirements, the Supplier shall work with Highways England to impact assess the effort required to design and deliver the new functionality through the Change and Release Management process.  |
|  | **15.**  | **File Services** 15.1 The WinTel Supplier shall provide File Services in accordance with the Customer’s information management policy. 15.2 In providing the File Services the WinTel Supplier shall: 15.2.1 enable Users to read/write and manipulate files on both personal and shared storage areas. Personal and shared storage shall be capable of handling all formats, file and entity types; 15.2.2 specify and manage access to personal storage, which shall be limited to the specific User and their authorised delegates; 15.2.3 incorporate changes to the File Services in accordance with changes to the Customer’s information management policy. 15.3 The WinTel Supplier shall provide functionality to encourage Users to store data and files in the corporate Electronic Document and Records Management System (EDRMS) and to use this as the main repository for documentation. 15.4 The WinTel Supplier shall liaise with the Customers' Hosting Supplier(s) to enable backup and restore of data associated with User data in accordance with the Customers' Service Operations Manual. 15.5 The WinTel Supplier shall provide reports specific to email and storage including data storage utilisation for: 15.5.1 Group Shares; 15.5.2 Local Office Data Shares; 15.5.3 Home Folders; 15.5.4 Email Private and Public Storage 15.6 The WinTel Supplier shall provide advice to Highways England where an email or data storage related action is recommended (e.g. email or file deletion).  |
|  |  16.  | **Messaging Services (Email)** 16.1 The Customer is in the process of implementing Office 365 including Exchange Online as part of the Modernising  |

|  |  |  |
| --- | --- | --- |
|  |  | Workplace project. This will result in a hybrid Exchange configuration, with some users on Exchange Online, and others using Exchange via the Customers’ Hosting Services environment.  |
|  |  16.2  | The WinTel Supplier shall provide an Email Service which includes as a minimum: 16.2.1 sending and receipt messages from the Internet; 16.2.2 sending and receipt of message from within Government networks (currently PSN); 16.2.3 attach/detach of files in industry standard formats with no loss of message or file integrity; 16.2.4 message text formatting functions (e.g. bold, underline, block moves, highlighting, bullet lists etc.); 16.2.5 address re-assignment functions (e.g. address book is transparent to physical location or sender and recipients); 16.2.6 choice of notification modes (e.g. automatic, manual) for incoming and outgoing message receipt, and message opened at destination; 16.2.7 notifications linked to message (e.g. to enable direct callup of related message); 16.2.8 automatic reply functions (e.g. pre-set reply message when away separate for internal versus external audiences); 16.2.9 individual calendars; 16.2.10personal contacts; 16.2.11notes; 16.2.12tasks; 16.2.13shared email and calendars; 16.2.14transfer of file attachments up to a maximum size per message as notified by the Customer from time to time.  |
|  | 16.3  | The WinTel Supplier shall provide an email archiving service using recognised industry supported solutions that are searchable and allow retention policies and archiving rules to be centrally administered  |
|  | 16.4   | The WinTel Supplier shall ensure that the Customer’s Electronic Document and Records Management System (EDRMS) components are loaded to enable emails and attachments to be stored, archived and organised in accordance with the Customer’s information management policies.  |

|  |  |  |
| --- | --- | --- |
|  | **17.**  | **Print Services** 17.1 The WinTel Supplier shall support the Print Supplier to provide a Print Service to provide Users access to printing facilities provided by other IT Suppliers in accordance with Customers policies and 3rd party contracts. 17.2 The WinTel Supplier shall manage the print queue for the print services supplied by other IT Suppliers.  |
|  |  **18.**   | **Productivity Tools** 18.1 The Customer owns the licenses for the standard Microsoft Office Productivity Services and the WinTel Supplier shall be responsible for the deployment, management and support of those Services to the business. Office 365 (including Skype for Business) will be provided to all users as part of the Modernising Workplace project. 18.2 The WinTel Supplier shall ensure that the End User Devices have a Web Browser Services. The Web Browser Services shall be compatible with various versions of Web Browser including Internet Explorer, Edge, Chrome and Firefox. 18.3 The WinTel Supplier shall facilitate the distribution of default User templates as necessary or required by the Customer. These shall allow the standardisation of Customer activity. 18.4 The WinTel Supplier shall ensure that the Customer’s Electronic Document and Records Management System (EDRMS) components are loaded into the Office Productivity suite to enable productivity documents to be stored, archived and organised in accordance with the Customer’s information management policies. 18.5 The WinTel Supplier shall provide a packaging and deployment Service for the Office productivity tools. 18.6 The Customer shall procure all required licenses and provide the required approval for users to have licenses deployed by the Supplier.  |
|  | **19.**  | **Remote Access** 19.1 The WinTel Supplier shall enable authorised Users to securely access Customer Applications from End User Devices whilst outside the corporate boundary via an HMG accredited Remote Access (RA) Service. The RA Service will be delivered in conjunction with the PSN Connectivity IT Supplier (who will own overall responsibility relating to RA).  |

|  |  |  |
| --- | --- | --- |
|  |  | 19.2 The WinTel Supplier shall work with the Connectivity IT Supplier to configure and integrate EUC Device allowances with appropriate RA client software to: 19.2.1 authenticate, authorise, monitor and log Users accessing Customer resources from outside the Customers corporate boundary; 19.2.2 monitor and audit remote activity to detect data leakage, malicious activity, use in contravention to the Customer’s policies or attempts to subvert the service; 19.2.3 record and account for User activity including the resources accessed, logon events, logoff events, logon attempts, timestamps, User identities, machine identities, token identities where available and any access attribute that can be logged; 19.2.4 provide reportable audit information to assure the remote access controls are operating in accordance with the Customer’s policies; 19.2.5 preserve the confidentiality of communications between the End User Device and the access service; 19.2.6 incorporate a capability to securely deliver Applications and resources of all types via a brokered model.  |
|  |  **20.**  | **Impact Assessments** 20.1 The Customer uses a process referred to as an Impact Assessment. This provides the Customer the ability to send work packages through to suppliers to evaluate and offer costs for the delivery of works and timescales entailed. 20.2 The WinTel Supplier shall complete and return the Impact Assessment within five working days as per the normal business hours (0700hrs – 1900hrs, Monday – Friday). Responses to Impact Assessments will be measured as an KPI. 20.3 The WinTel Supplier shall provide associated costs for the resources required to implement works if beyond the availabilities of the personnel already assigned to the delivery of Service. Costs for the inclusion of Capital Expenditure required to procure tools/products, must be included.  |
|  | **21.**  |  **Citrix Management**  |

|  |  |  |
| --- | --- | --- |
|  |   | 21.1 The Customer currently provides a Citrix environment (running on Windows 2012 R2) accessed by both internal users and external partners. 21.2 The WinTel Supplier shall provide a fully managed service for packaging and deploying Citrix software for all in scope End User Devices including tablets, using the provided Citrix environment in line with the Application Packaging conditions of this contract. 21.3 The WinTel Supplier shall work with the IT Supplier responsible for the Citrix platform to ensure users have the required level of access to applications published within the Citrix platform from their End User Device where appropriate.  |
|  | **22.**   | **ITIL Aligned Best Practice** 22.1 The Supplier is expected to deliver the Service in alignment with ITIL best practice  |
|  | **23.**  | **Demand Management** 23.1 The WinTel Supplier shall provide Demand Management for the EUC Services, including: 23.1.1 Developing EUC Service demand models and demand forecasts based on Patterns of Business Activity provided by the Customers Service Management Supplier; 23.1.2 making recommendations to reduce demands on EUC Services; 23.1.3 making recommendations on how Capacity Plans are/shall be affected by demand projections including the steps needed to meet demand projections; 23.1.4 support the Customer and Service Management Supplier in making available to the Customer's business units the mechanisms in place to control demand for EUC Services; and 23.1.5 making recommendations to the Customer and Service Management Supplier for improvements of the mechanisms to control and meet current and forecast demand for EUC Services. 23.1.6 The WinTel Supplier shall report on demand trends for EUC Services with the purpose of identifying and reporting risks inherent in demand forecasts and capability to meet demand.  |

|  |  |  |
| --- | --- | --- |
|  |  **24.**   | **Financial Management** 24.1 The WinTel Supplier shall provide EUC Service financial data to the Customer in accordance with the Financial Management Policies, Processes and Procedures. 24.2 The WinTel Supplier shall provide EUC Service consumption data to the Service Management Supplier in accordance with the Service Operations Manual. 24.3 The WinTel Supplier shall support the Service Management Supplier in resolving any discrepancies in EUC Service consumption data.  |
|  | **25.**   | **Service Portfolio Management** 25.1 The WinTel Supplier shall manage the EUC Service Portfolio to ensure EUC Services are current and meet business needs. 25.2 The WinTel Supplier shall support the Service Management Supplier to produce, maintain and provide the IT Services Portfolio, including identifying the optimal mix of EUC Services required to deliver the IT Services. 25.3 Where new business requirements identify the need for additional EUC Services, these shall be impact assessed to determine the effort to deliver the new business requirement through the EUC Service.  |
|  | **26.**  | **Service Risk Management** 26.1 The WinTel Supplier shall identify and mitigate any emergent risk to the provision of EUC Services. 26.2 The WinTel Supplier shall advise the Service Management Supplier of any emerging risks and shall provide a proposal of how such emerging risks should be addressed in accordance with the current ITSCM (IT Service Continuity Management) Plan, where this exists and the Information Security Management Plan and ITSCM Policies and Procedures 26.3 The WinTel Supplier shall implement any measure identified to address any emerging risk which has been approved by the Customer under the direction of the Service Management Supplier. Such measures shall be implemented in accordance with the Service Request Process.  |
|  |  **27.**  | **Availability Management**  |

|  |  |  |
| --- | --- | --- |
|  |  | 27.1 The WinTel Supplier shall produce an availability plan and (where appropriate) an availability improvement plan in accordance with the Availability Management Policies, Processes and Procedures. 27.2 The WinTel Supplier shall participate in regular availability risk reviews under the direction of the Service Management Supplier. 27.3 The WinTel Supplier shall support the Service Management Supplier to schedule and coordinate any Planned Outages in accordance with the Availability Management Policies, Processes and Procedures in order to minimise disruption to Patterns of Business Activity. 27.4 The WinTel Supplier shall collect, analyse and maintain availability data and report on that data for EUC Services. Availability management reporting shall include availability, reliability, and maintainability. 27.5 The WinTel Supplier shall identify and rectify problem areas which impact or have the potential to impact availability. 27.6 The WinTel Supplier shall assess the impact of planned changes against availability plans. 27.7 The WinTel Supplier shall identify tactical and strategic risks to availability in the medium- to long-term and prepare mitigation plans. 27.8 The WinTel Supplier shall, working with the Service Management Supplier, ensure the delivery of EUC Services meet agreed availability, design criteria and Service Levels  |
|  |  **28.**  | **Capacity Management** 28.1 The WinTel Supplier shall produce and maintain Capacity Plans for the EUC Services that cater for: 28.1.1 fluctuations in business as usual capacity demand; 28.1.2 planned business change; 28.1.3 patterns of Business Activity; 28.1.4 revised or new Service Levels; 28.1.5 revised or new EUC Services; 28.1.6 ITSCM; 28.1.7 transition requirements; 28.1.8 the impact of emerging technologies within the Service pipeline. 28.2 The WinTel Supplier shall advise the Service Management Supplier of predicted capacity shortfalls and propose solutions,  |

|  |  |  |
| --- | --- | --- |
|  |  | impact, risks and cost, providing supporting evidence on a timely basis as needed. 28.3 The WinTel Supplier shall translate Patterns of Business Demand to EUC Service demand and provide forecast EUC Service demand to the Service Management 28.4 The WinTel Supplier shall take appropriate action or make recommendations to relieve capacity restrictions beyond agreed thresholds. 28.5 The WinTel Supplier shall proactively report on resource capacity and resource utilisation. 28.6 The WinTel Supplier shall recommend appropriate capacity thresholds in accordance with the Service Levels and the Capacity Management Policy 28.7 The WinTel Supplier shall optimise resource utilisation in a costeffective manner (Resource Capacity Management). 28.8 In the event that there are discrepancies between the EUC Service consumption information provided by the WinTel Supplier, the WinTel Supplier shall work with the Service Management Supplier to resolve such discrepancies 28.9 The WinTel Supplier shall work with the Service Management Supplier to facilitate the optimisation of Capacity and increase or decrease Capacity for the EUC Services in order to maintain the operation of the IT services  |
|  |  **29.**  | **IT Service Continuity Management (ITSCM)** 29.1 The WinTel Supplier shall provide input into IT Service Continuity Management plans in accordance with the Service Operations Manual. 29.2 The WinTel Supplier shall provide a single point of contact for Business Continuity and Disaster Recovery planning, related communications and other activities within the scope of the EUC Services. This single point of contact shall be identified as a Key Person. 29.3 The WinTel Supplier shall document and maintain priorities for backups, Disaster Recovery and Business Continuity where applicable to the EUC Wintel Services, based on the Customer’s business continuity requirements. 29.4 The WinTel Supplier shall manage Service Continuity risks for EUC Services, including maintaining descriptions of possible and high probable crisis situations and incorporating mitigation  |

|  |  |  |
| --- | --- | --- |
|  |   | and contingency actions into the ITSCM Plans (scenario planning). 29.5 The WinTel Supplier shall collaborate with the Service Management Supplier to develop an agreed set of ITSCM Plans in accordance with the Service Operations Manual. 29.6 The WinTel Supplier shall take part in ITSCM Awareness and Training for ITSCM related personnel as part of the ITSCM lifecycle. 29.7 The WinTel Supplier shall support the Service Management Supplier and the Customer in the production of Business Impact Analysis as and when required by the Customer. 29.8 The WinTel Supplier shall comply with any improvements which need to be made to the ITSCM Plans. 29.9 The WinTel Supplier shall ensure that the management and reporting of the EUC Services and components thereof are configured in a way that ensures the information captured can be used in planning IT Service Continuity for the IT services.  |
|  | **30.**   | **Service Catalogue Management** 30.1 The WinTel Supplier shall develop, maintain and make available to the Service Management Supplier the Service Catalogue to ensure that it is always current with the EUC Services. 30.2 The WinTel Supplier shall develop, maintain and make available the Requestable EUC Services via the Requestable Services Catalogue, including: 30.2.1 details of all available Requestable Services and components thereof (e.g. Software, Hardware); 30.2.2 details for how Users can request applicable EUC Services; 30.2.3 information relating to Requestable EUC Services that is easily understandable by any User; 30.2.4 authorisation and Escalation Procedures and contacts; 30.3 The WinTel Supplier shall agree and document Service Definitions and all documentation (as detailed in the Policies and Procedures) for Requestable EUC Services with the Service Management Supplier. 30.4 The WinTel Supplier shall maintain the appropriate Service Assets and Configuration Items for all EUC Service Catalogue Items.  |
|  | **31.**  | **Service Level Management**  |

|  |  |
| --- | --- |
|  | 31.1 The WinTel Supplier shall provide and deliver the EUC Services to the agreed availability and design criteria and propose Service Levels, Service Level Targets and Key Performance Indicators for new or changed EUC Services in a timely manner. 31.2 The WinTel Supplier shall provide all relevant information relating to Service Levels, Service Level Targets and Key Performance Indicators for the EUC Services. 31.3 The WinTel Supplier shall participate in negotiations to ensure all Service Levels for EUC Services are appropriate and in line with the IT Service Levels. 31.4 The WinTel Supplier shall demonstrate Service Levels as part of Service Validation for the purpose of determining whether the expected service performance is achievable. 31.5 The WinTel Supplier shall support the Service Management Supplier in the analysis of EUC Service performance to ensure completeness and appropriateness of content for presentation to the Customer. 31.6 The WinTel Supplier will produce a monthly report for discussion as part of a monthly Governance review. The report will detail key elements of the service, SLA conformance and continual service improvements. 31.7 The WinTel Supplier will seek to achieve the following SLAs  |
|  | Service Level  | Service Level Target  | Service Credit  |
| Email Availability  | 99.5%, calculated as 100% minus the ratio of email Service Hours (24x7x365) where email is unavailable e due to Incidents or other issues within the scope of the EUC Services against the total number of email Service Hours. For the avoidance of doubt, email availability is defined as the ability of a user to (a) access and retrieve information from the mail server, and (b) send and receive messages via the mail server, provided their account is active and enabled Availability will be calculated on outages that impact 10 users or more and will exclude planned maintenance. This is users with logged calls for isolated events, or categorised as all users on a specific Exchange Server for Server events. Mailboxes migrated to O365 are excluded from the availability measurement as this will be dependent on the Microsoft Exchange Online platform’s availability.  | 2%  |
| Configuration Management  | 98% accuracy of all Configuration Items under the Supplier’s management.  | 0%  |



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | End User Device Availability  | KPI for no more than 3% of users have a logged WinTel incident on their EUC Device within a monthly period.  | 0%  |
| End User Device Performance  | KPI to show average login time from the point of power-up to the completion of all start-up activities  | 0%  |
| Software Distribution  | 98% of End User Devices are operating the correct versions of all applicable Software, which is anti-virus software, detection signature updates (within 24 hours of release by the vendor) and critical security patches/updates (within 7 days of release by the vendor) providing that the End User Device is connected to the network and agreed web browsers  | 0.5%  |
| Upgrade notification (KPI)  | 98% of software upgrades are notified to the Highways England Service Management team within 5 days of release. The software list is limited to Antivirus, OS patches and upgrades, Adober Reader, Microsoft Office and agreed Web browsers  | 0%  |
| Print Availability  | 99.90% availability for print job spooling and transmission at all Customer Premises standard opening hours (0700 – 1900 Monday – Friday for main officers, 24hrs x 7 days for RCCs, NTOC etc, excluding agreed Planned Outages). Availability excludes any devices that are not managed by the Win Tel supplier.  | 2%  |
|  31.8 If the Supplier does not achieve an SLA, then remediation steps will be defined and tracked to achieve ongoing conformance. 31.9 The Customer reserves the right to review and where applicable amend the SLA’s with the WinTel Supplier every 6 months from commencement of the contract. 31.10 The WinTel Supplier will seek to achieve the KPI of, accurately responding to Impact Assessment within 5 working days.  31.11 2nd year reduction in Service Charge: 31.11.1For year 2 of the Service, a reduced monthly charge will apply. 31.11.2The WinTel Supplier will work with Highways England to rationalise the service to allow the reduced profile and support the transition of services into Highways England to be effective. If SLA conformance is at risk, then both parties may agree a varied profile if required.    |

|  |  |  |
| --- | --- | --- |
|  |  **32.**    | **Service Level Details and Measures** 32.1 The objectives of these Service Level Agreements are to: 32.1.1 ensure that the Services are of a consistently high quality and meet the Service Levels and other requirements of Highways England; 32.1.2 provide a mechanism whereby the Service Levels, Key Performance Indicators (KPIs) and Service Credits can be modified over the Contract Period in response to the changing requirements of Highways England; and 32.1.3 incentivise the WinTel Supplier to: 32.1.3.1meet the Service Levels and KPIs; 32.1.3.2promptly rectify any failure to meet the Service Levels or KPIs. 32.2 **Service Level and KPI Principles** 32.2.1 Any failure by the WinTel Supplier to deliver the Services, and to achieve the Service Levels and KPIs will have an impact on Highways England’s operational effectiveness and efficiency and subsequently its ability to fulfil its statutory obligations. 32.2.2 The Service Levels and KPIs are focussed on Highways England; reflect the needs of Highways England and represent the Services quality that is required by Highways England and its business units and end users. 32.2.3 The WinTel Supplier shall work collaboratively with other Highways England IT Suppliers to deliver the ICT Services and ensure that the Service Levels and KPIs are met. 32.3 The objectives of the Service Credits and other related remedies are to: 32.3.1 ensure that the Services are of a consistently high quality and meet the Service Levels and other requirements of Highways England; 32.3.2 use Service Credits as a method of price adjustment to reflect poor performance in breach of the required Service Levels; 32.3.3 provide a mechanism whereby the Service Credit regime can evolve over the Contract Period as the profile of Services change; and  |

|  |  |  |
| --- | --- | --- |
|  |  | 32.3.4 incentivise the Supplier to meet the Service Levels and work to remedy any failure to meet the Service Levels promptly. 32.4 The WinTel Supplier acknowledges that Highways England will, in all cases, prefer to receive the Services at the Service Level Target in preference to receiving the Service Credits. Consequently the Supplier shall, in all cases, seek to deliver the Services at or above the Service Level Target in preference to accepting a liability for Service Credits. 32.5 The Supplier shall be open, transparent and honest about the levels of performance and service quality the Supplier is achieving with Highways England and the Tower Service Suppliers.  |
|  | **33.**  |  **Service Level Framework** 33.1 The table in Paragraph 31.7 (above) sets out the Service Level Target that shall be measured and reported on by the Supplier, including the Service Level Targets and associated Service Credits. 33.2 On a 6 monthly basis, Highways England and the Wintel Supplier will meet to review the Service Levels and KPIs, and any associated Service Credits, and in addition on reasonable request from Highways England or Netcompany in accordance with paragraph 33.4 below. 33.3 All KPIs that will be reported on by the Supplier alongside the Service Levels will be agreed between the WinTel Supplier and Highways England, and reported on monthly. 33.4 In the event that: 33.4.1 any Services or component thereof, does not achieve the Service Level Targets, KPIs or any other agreed performance measures, Highways England Representative or Netcompany reserves the right to invoke a review of the Service Levels (including Service Level Targets) and KPIs; 33.5 Without prejudice to the provisions of the Change Control Procedure, the Supplier shall co-operate with any review of Service Levels undertaken in accordance with the provisions of paragraphs 33.2 or 33.4. The Supplier shall not unreasonably withhold agreement to the introduction of new Service Levels or the amendment of existing Service Levels.  |

|  |  |  |
| --- | --- | --- |
|  |  | 33.6 Any change in Service Levels or associated Service Credits shall be subject to the Change Control Procedure. 33.7 Immediately following each anniversary of the Operational Services Commencement Date, the Supplier shall submit proposed improvements to the Service Levels (such as improved Service Level Targets) for the following 12 months in order to support the requirement for continuous improvements in its performance. 33.8 If the Achieved Service Level does not meet the applicable Service Level Target, then Service Credits will be due from the Supplier in accordance with Paragraph 3.  33.9 All Service Level Targets shall be measured over a Service Period, which unless otherwise specified in writing by Highways England, shall be a calendar month.   |
|  | **34.**  | **SERVICE CREDIT CALCULATION** 34.1 For each Service Level, the Service Credit is determined by the Achieved Service Level, and the Service Level Target.34.2 Where the Achieved Service Level is at or above the Service Level Target, Service Credit %= 034.3 Where the Achieved Service Level is below the Service Level Target, Service Credit % is as described in the SLA table, calculated as a % of the monthly Service charge for the EUC WinTel Service. 34.4 Unless stated otherwise in this document, the Service Credit (£) is calculated by **Service Credit (£) = Service Credit (%) x Service Contract Charge for the Service Period.** 34.5 Service Credits are cumulative within a Service Period, however, should multiple service credits be linked to the same incident, then only the highest service credit shall apply. 34.6 Aggregate Service Credits for all Services delivered by the Contractor to Highways England shall be limited in each Service Period to fifteen percent (15%) of the aggregate Charges payable to the Supplier within the same Service Period and subject to an annual cap of 10% of the annual Service Charge. 34.7 Highways England may use the Management Information to, among other things, verify the calculation and accuracy of the Service Credits, if any, applicable to each relevant Service Period.  |

|  |  |
| --- | --- |
|  | 34.8 Service Credits are a reduction of the amounts payable in respect of the Services and do not include VAT. The Supplier shall set-off the value of any Service Credits against the next appropriate invoice in accordance with the provisions of this Contract.   1. **REPEAT FAILURES TO MEET SERVICE LEVEL TARGETS**
	1. If the WinTel Supplier fails to achieve a Service Level Target in a Service Period and then fails to achieve the same Service Level Target in a subsequent Service Period, the failure in the subsequent Service Period shall be a **“Repeat Failure”**. The Repeat Failure count shall increment by one (1) for each additional failure.
	2. The Repeat Failure count shall be reset to zero (0) once there have been two (2) consecutive Service Periods in which the Service Level Target has been met.
	3. A worked example is set out below:

  |
|  |   | **Service Period**  |
|   | **1**  | **2**  | **3**  | **4**  | **5**  | **6**  | **7**  | **8**  | **9**  | **10**  | **11**  | **12**  |
| Failure to meet Service Level Target for a Service (F)  | F  | F  |   | F  |   |   | F  |   | F  | F  |   | F  |
| No. of Repeat Failures  | 0  | 1  |   | 2  |   |   | 0  |   | 1  | 2  |   | 3  |
|  *Table 1 Repeat Failure Example*  35.4 For any failure to meet Service Level Targets which is a Repeat Failure, the Service Credit applicable shall be increased as follows (a “**Repeat Failure Multiplier**”):   |
|  | **Repeat Failure count applicable to the Service Period**  | **Repeat Failure** **Multiplier**  |  |
| 0  | 1  |
| 1  | 1.25  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | 2  | 1.5  |  |
| 3 and above  | 2  |
| *Table 2 Repeat Failure Multipliers*  |
|  | **36.**  | **Service Levels Reporting And Management Information** 36.1 For the Service Levels that apply to the ICT Services, as defined in Annex A of this Schedule, and the KPIs that apply to the ICT Services, the Supplier shall report on the measurement and management of these Service Levels and KPIs. 36.2 The WinTel Supplier shall provide Management Information and Service Credit calculations in an aggregated form to Highways England based on its own records. The Management Information may include, but shall not be limited to, such of the following as Highways England Representative shall specify: 36.2.1 Availability of the ICT Services in the WinTel Supplier’s scope; 36.2.2 Application performance management; 36.2.3 Resolution targets for Incident management; 36.2.4 Resolution targets for service request management; and 36.2.5 Service Level Targets, or activities or tasks that make up a Request For Service. 36.3 All Management Information and reports that are to be submitted to Highways England for a Service Period will be agreed between Highways England and the WinTel Supplier.   |
|  | **37.**  | **Management and Escalation of Service Level Failures** 37.1 Introduction 37.1.1 The procedures set out in this Section are intended to enable the Supplier to manage service issues arising from failure to achieve the Service Levels. 37.1.2 The Service Credit provisions of this Schedule shall continue to apply throughout any escalation process. 37.1.3 The WinTel Supplier shall proactively resolve outstanding issues relating to Services availability and performance and raise awareness of any matters that have, or may have, a material impact on the availability or performance of the Services. 37.1.4 Where further remedial action is required or where reasonably required by Highways England Representative, the WinTel Supplier shall provide a  |

|  |  |
| --- | --- |
|  | Recovery Plan for the approval of the Highways England Representative. The scope and format of all Recovery Plans shall be agreed with Highways England.  1. **Supplier Management**
	1. The WinTel Supplier shall work under the direction and management of the Service Management Supplier and shall comply with the Service Operations Manual in the operational delivery of the EUC Services.
	2. The WinTel Supplier shall support the Service Management

Supplier in the development and maintenance of the Service Operations Manual to ensure that the EUC Services effectively interface with the ITIL processes and IT Services. * 1. The WinTel Supplier shall address any non-compliance with the Service Operations Manual whether identified by the Service Management Supplier or otherwise.
	2. The WinTel Supplier shall work with the Service Management

Supplier to develop and implement Operational Level Agreements and treat the Service Management Supplier and other IT Suppliers equally and impartially, and shall deal with the Service Management Supplier and IT Suppliers professionally, courteously and openly with the intention of achieving effective working relationships to deliver the best possible IT services. * 1. The WinTel Supplier shall continually monitor and optimise the EUC Services.
	2. The WinTel Supplier shall notify the Service Management Supplier as soon as they become aware of any issue or potential issue and provide proposals of how to address such issues.
	3. The WinTel Supplier shall provide information for the EUC Services and components thereof in accordance with the

Service Operations Manual. Where any major change may bring significant benefit to the buyer the Supplier will raise this for possible impact as a form Change for impacting and implementation.  **Service Transition**  1. **Transition Planning and Support**
 |

|  |  |  |
| --- | --- | --- |
|  |  | 39.1 The WinTel Supplier shall provide Transition Services in line with the approach and plan submitted as part of the Suppliers tender documents. 39.2 The WinTel Supplier shall support the Service Management Supplier to assess risks to service failure and disruption through Transition and ensure that these have been understood and agreed with the Customer and that mitigating actions are in place with appropriate control and management in accordance with the Risk Management Policies and Procedures. 39.3 The WinTel Supplier shall support the creation of Early Life Support Plans as directed by the Customer and shall address any issues identified by the Service Management Supplier through assurance of Early Life Support Plans 39.4 The WinTel Supplier shall maintain the integrity of in situ EUC Service Assets, Configuration Items, Services and components thereof during the course of Transition and shall update the CMDB as necessary 39.5 The WinTel Supplier shall update the CMDB and operational procedures as necessary to undertake effective management, delivery and support to the use and consumption of the new or changed EUC Services by the Customer.  |
|  |  **40.**  | **Change and Evaluation Management** 40.1 The WinTel Supplier shall cater for all categories of EUC Change under the direction of the Service Management Supplier, including: 40.1.1 Operational Change requests; 40.1.2 Standard (pre-approved) Change requests e.g. via the Requestable Service Catalogue; 40.1.3 Emergency Change requests. 40.2 The WinTel Supplier shall schedule, plan assess and implement Changes in accordance with the Service Operations Manual. 40.3 The WinTel Supplier shall participate in Change Management Board, Operational Change Advisory Board, and Post Implementation Reviews in accordance with the Service Operations Manual. 40.4 The WinTel Supplier shall assess the impact of Changes on the EUC Services including: 40.4.1 Verified Implementation Plans; 40.4.2 Post Implementation Review; 40.4.3 Acceptance Criteria;  |

|  |  |  |
| --- | --- | --- |
|  |   | 40.4.4 Back Out Plans or Remediation Plans; 40.4.5 Plans for handover to support. 40.5 The WinTel Supplier shall update the CMDB and all relevant documentation in respect of all EUC Service Assets and Configuration Items included in a Change as part of the execution of a Change, in accordance with the Service Operations Manual and such that the CMDB is at all times, an accurate reflection of the physical and logical implementation of the Services. 40.6 Where any Change is simply not implementable without impact to day to day support, based on its size and effort required, this will be costed and impacted as a formal Change. 40.7 The WinTel Supplier shall implement all approved Changes; and shall not implement Changes that have not been properly authorised in accordance with the Service Operations Manual.  |
|  | **41.**  | **Knowledge Management** 41.1 The WinTel Supplier shall maintain and regularly update the Knowledge Database with Supplier solutions and best practices as they are developed, including updates based on “lessons learned”. 41.2 The WinTel Supplier shall update a Service Knowledge Management System (SKMS) in collaboration with the Service Management with data and information on the EUC Services including but not limited to: 41.2.1 Methods to resolve Incidents; 41.2.2 Known Errors; 41.2.3 Service Desk scripts; 41.2.4 Self-help articles; and 41.2.5 Frequently asked questions (FAQs). This will be stored in the Customers instance of ServiceNow. 41.3 When data relating to the EUC Services is found in the SKMS that is inaccurate, incomplete or lacks integrity, the WinTel Supplier shall correct or remove such data. 41.4 The WinTel Supplier shall cooperate with the Service Management Supplier and the Customer to carry out conformance reviews and audits from time to time to ensure the integrity and accuracy of data in the SKMS.  |
|  |  **42.**  | **Release and Deployment Management**  |

|  |  |  |
| --- | --- | --- |
|  |  | 42.1 The WinTel Supplier shall under the direction of the Service Management Supplier provide input as required into all Release activities for the EUC elements, including but not limited to: 42.1.1 Release Plans; 42.1.2 Release Packages; 42.1.3 Implementation activities.  |
|  |  **43.**  | **Service Asset and Configuration Management** 43.1 The WinTel Supplier shall work with the Service Management Supplier to ensure that the CMDB provides a single view of all EUC Service Assets and Configuration Items. For the avoidance of doubt this includes undertaking any activities necessary to integrate their own processes with and create the necessary interfaces to the Service Management Supplier’s ITSM Toolset providing the CMDB implemented is deemed fit for purpose. 43.2 The WinTel Supplier shall mange the identification, recording and maintenance of attributes of and relationships between Configuration Items (CIs) under the management of the WinTel Supplier, including relationships to Configuration Items that are managed by other IT Suppliers, and shall update the CMDB whenever changes to EUC CI's or any of their attributes are made providing the CMDB implemented is deemed fit for purpose. 43.3 The WinTel Supplier shall address all CI Exceptions regarding EUC Configuration Items and ensure that remedial actions are implemented following any CI Exception. 43.4 The WinTel Supplier shall provide status accounting and reporting for assets, configuration items and their attributes in accordance with the Service Operations Manual. 43.5 The WinTel Supplier shall record all attributes of EUC Assets in collaboration with the Service Management and in accordance with the Service Operations Manual. 43.6 Should the WinTel Supplier identify inactive EUC Assets in accordance with the Customer’s Asset Management Policy, the WinTel Supplier shall coordinate the removal or reallocation of such EUC Assets in accordance with the Service Operations Manual and the Lifecycle Management Service.  |
|  |  **44.**  | **Service Validation and Testing** 44.1 The WinTel Supplier shall participate in Testing for EUC elements as directed by the Customer including Integration  |

|  |  |
| --- | --- |
|  | Testing, Operational Acceptance Testing and Service Acceptance Testing 44.2 For any project activity or significant Change if such Testing will impact day to day support and SLA achievement this will be flagged and subject to impact.  **Service Operations**  1. **Access Management**
	1. The WinTel Supplier shall manage access to the IT Services through the Active Directory (SSO and MetaDirectory) Service. For the avoidance of doubt the Service Management Supplier shall provide password management and user account creation services through the IT Suppliers.
	2. The WinTel Supplier shall provide access to the EUC Services in accordance with the User Administration Policy and the Service Operations Manual.
	3. The WinTel Supplier shall ensure that all changes to access comply with the User Administration policy and the Service Operations Manual.
	4. The WinTel Supplier shall propose to the Service Management Supplier and IT Suppliers mechanisms to efficiently manage the granting of authorisation to Users and the management of lists of authorised Users through the Active Directory (SSO and MetaDirectory) Service.

 1. **Event Management**
	1. The WinTel Supplier shall log, track, filter, aggregate and associate EUC Events in accordance with the Service Operations Manual and shall provide automated alarms and indication of Incidents to the Service Management Supplier when thresholds are exceeded.
	2. The WinTel Supplier shall investigate in conjunction with the Service Management Supplier and other IT Suppliers the resolution of exceptional or abnormal Events that have reached a threshold or met certain criteria in accordance with the Service Operations Manual.
	3. The WinTel Supplier shall support the Service Management Supplier in the determination of EUC Event thresholds and shall set and adjust Event thresholds as directed by the Service Management Supplier.
 |

|  |  |  |
| --- | --- | --- |
|  |  **47.**  | **Incident Management** 47.1 The WinTel Supplier shall investigate and resolve Incidents allocated to it by the Service Management Supplier in accordance with the Service Levels, including: 47.1.1 assess the probable cause of an EUC hardware fault; 47.1.2 replace or repair faulty equipment, as appropriate, procured by Highways England; 47.1.3 power-up and carry out scripted function testing; 47.1.4 restore the equipment to its appropriate configuration; 47.1.5 test the replaced or repaired equipment to ensure it is functioning correctly. 47.2 The WinTel Supplier shall notify the Service Management Supplier promptly of any Incident of which it becomes aware other than through allocation from the Service Management Supplier. 47.3 `The WinTel Supplier shall proactively notify the Service Management Supplier of any Incident that is known to be in breach or highly likely to create a P1 or P2 or that has, in the opinion of the WinTel Supplier, been incorrectly allocated. 47.4 The WinTel Supplier shall update the Incident record with all relevant information relating to the Incident and shall update Known Error information in the SKMS in relation to Incidents. 47.5 The WinTel Supplier shall launch further investigation and action as required in relation to Incident trends.  |
|  |  **48.**   | **Problem Management** 48.1 The WinTel Supplier shall provide a Problem Management Service that proactively seeks to prevent Incidents from happening within the EUC Services, and minimise the impact of Incidents that cannot be prevented. 48.2 The WinTel Supplier shall analyse, monitor, progress, resolve and review Problems in line with the Service Levels and the Service Operations Manual. 48.3 The WinTel Supplier shall provide Problem analysis and management information to the Service Management Supplier including, but not limited to, information relating to Problem trends, volumes and Problem solutions.  |
|  | **49.**  | **Service Request Fulfilment**  |

|  |  |
| --- | --- |
|  | 49.1 The WinTel Supplier shall fulfil Service Requests allocated to it by the Service Management Supplier in accordance with the Service Levels, including identifying and notifying the Service Management Supplier of any Service Requests that require Customer approval or action, raising of supplementary tasks or Change Requests, creation of Projects, or raising of Contract Changes. 49.2 The WinTel Supplier shall respond to enquiries regarding Service Requests with accurate and up-to-date information. 49.3 The WinTel Supplier shall provide early notification of any potential breach of Service Levels relating to P1 or P2 Service Requests to the Service Management Supplier. 49.4 The WinTel Supplier shall provide to the Service Management Supplier accurate and up-to-date management information regarding Service Requests including but not limited to volumes, trends and categories within each Service Reporting Period. 49.5 The WinTel Supplier shall proactively monitor Service Requests to ensure that multiple and/or linked Service Requests are fulfilled in the most expedient and efficient manner to minimise business disruption.  **Continual Service Improvement** 1. **Identify and Deliver Service Improvements**
	1. The WinTel Supplier shall identify and notify to the Service Management Supplier process improvements and recommendations for consideration in respect of the EUC Services.
	2. The WinTel Supplier shall through continual improvement and by working together with the Service Management Supplier and other IT Suppliers and the Customer manage the reduction in volume of Incidents and Problems over the Term.
	3. The WinTel Supplier shall produce, maintain and provide to the Service Management Supplier a EUC Service Improvement Plan in accordance with the Service Operations Manual.
	4. The WinTel Supplier shall deliver service improvements under the direction of the Service Management Supplier acting on behalf of the Customer in accordance with the agreed EUC

Service Improvement Plan and shall keep the Service  |

|  |  |
| --- | --- |
|  | Management Supplier informed on the progress against Service Improvement Plans. 50.5 The WinTel Supplier shall provide advice, guidance and support to the Service Management Supplier on the use of the Services. 50.6 The WinTel Supplier shall identify opportunities to improve the maturity of the EUC Services and their integration into the IT Services and shall manage the implementation of opportunities approved by the Service Management Supplier.  1. **Service Management and Performance Management**
	1. The WinTel Supplier shall measure, manage and report on the performance of the EUC Services in accordance with the Service Operations Manual and the defined Service Levels in a monthly report to Highways England.
	2. The WinTel Supplier shall ensure performance information provided shall contain, but is not limited to, details of
		1. performance over the agreed Service Reporting Period;
		2. provide details of service credits accrued during the Service Reporting Period separately;
		3. year to date; and
		4. show an aggregate of performance month on month over an 18 month period.
	3. The WinTel Supplier shall ensure the quality of source information for performance is complete, accurate and timely

 **Service Lifecycle Management**  1. **IT Service Management Toolset (ITSM)**
	1. The WinTel Supplier shall integrate its data, tools and processes

with the ITSM Toolset (ServiceNow) provided by the Customer, where appropriate and where there is a clear business benefit, in order to facilitate the efficient and timely delivery of the IT Services, including: * + 1. Availability Management Information System (AMIS)
		2. IT Capacity Management Information System (CMIS)
		3. Service Knowledge Management System (SKMS)
		4. Event Management System
		5. Incident Management System
		6. Problem Management System
		7. Customer Service Catalogue
		8. Change Management
 |

|  |  |  |
| --- | --- | --- |
|  |  | 52.1.9 Configuration Management Database (CMDB) 52.2 The WinTel Supplier shall comply with the ITSM Toolset’s Integration Standards and the Policies and Procedures for the maintenance, interfacing and update of the ITSM Toolset provided by the Customer. Interfaces and processes shall be defined in the Service Operations Manual  |
|  | **53.**  | **License Management and Compliance** 53.1 The WinTel Supplier shall manage appropriate auditing tools including software licensing which shall include automated monitoring, metering, removal and reassignment of Software on End User devices, subject to the toolset providing the required functionality. 53.2 The WinTel Supplier shall utilise the licences in the most costeffective manner available, while considering the business requirements. 53.3 The WinTel Supplier shall operate a Software discovery capability enabling reports to be provided to the Customer for all software installed on End User Devices. The reporting must include software usage metering and shall report the attributes as defined in the Service Operations Manual in order to enable the Customer to perform its legal, regulatory and contractual obligations. 53.4 The WinTel Supplier shall ensure that the Software discovery capability is kept up to date with the latest recognition patterns for all software installed on End User Devices. 53.5 The WinTel Supplier shall proactively monitor the use of all Software under the direction of the Service Management Supplier in order to maintain strict compliance, including: 53.5.1 immediately notifying and advising the Service Management Supplier of any Software license compliance issues identified within the End User environment or associated with the use of or support of the EUC Services; 53.5.2 software associated with the EUC Services; 53.5.3 identifying the presence of any unauthorised or nonstandard Software; 53.5.4 providing periodic reporting of license information and compliance to Service Management Supplier; and  |

|  |  |  |
| --- | --- | --- |
|  |  | 53.5.5 filing and tracking Software license agreements in the Service Portfolio and ensuring appropriate links within the CMDB, Asset Register and Definitive Media Library. 53.6 The WinTel Supplier shall provide Software usage reporting to enable the Customer to understand application usage by Users in order to be able to (amongst other things) rationalise usage.  |
|  |  **54.**  | **Customer Business Security Requirements** 54.1 The WinTel Supplier and the EUC Services shall comply with: 54.1.1 HMG Security Policy Framework (aligned with ISO 27001, found at https://www.gov.uk/government/publications/securitypolicy-framework) 54.1.2 PSN Code of Connection (PSN CoCo) found at https://www.gov.uk/public-services-network 54.2 The WinTel Supplier shall be able to communicate, store, transfer and process data on platforms accredited to handle the appropriate impact level associated with the EUC Services. EUC services are required to securely hold data at an Official – Sensitive level. 54.3 The WinTel Supplier shall comply with the Information Security Audit policies, procedures and compliance criteria contained in the Service Operations Manual. 54.4 The WinTel Supplier shall support the Service Management Supplier to conduct Information Security Audits at least annually in line with the Customer processes, procedures and compliance criteria for the EUC Services. 54.5 The WinTel Supplier shall produce and maintain compliance statements and supporting documentary evidence in line with the obligations documented in any code of connections. 54.6 The WinTel Supplier shall make available to the Customer any code of connection compliance report at least annually.  |
|  |  **55.**  | **End Point Protection** 55.1 The WinTel Supplier shall provide deployment and ongoing management and maintenance for an End Point Protection Service, such as but not limited to local disk encryption and antivirus protection through the use of the McAfee suite of tools currently deployed to the Windows 7 estate and Bitlocker and Windows GPOs for the Windows 10 estate. 55.2 In providing the End Point Protection Service, the WinTel Supplier shall:  |

|  |  |  |
| --- | --- | --- |
|  |  | 55.2.1 provide information and reports that demonstrates and assures the controls are operated to the standards set out in the Customer’s policies; 55.2.2 provide physical controls to prevent unauthorised physical access to EUC Assets where appropriate and under the control of the Supplier; 55.2.3 harden the device configuration to the Customer standards; 55.2.4 deploy and maintain anti-virus (AV) controls capable of detecting, preventing and removing malicious software; 55.2.5 where appropriate provide encryption of data on EUC Assets, digital signatures, non-repudiation and mutual or individual authentication through appropriate cryptographic controls; 55.2.6 detect and prevent the use of unauthorised attached peripherals such as but not limited to removable media, smartphones, tablets, media players and cameras; 55.2.7 detect and approve the use of authorised attached peripherals, as requested by the Customer and approved by the Customers’ Cyber Security team; 55.2.8 detect and prevent unauthorised file and object modification in Active Directory through appropriate integrity controls; and 55.2.9 detect and record security events and to pass those events in an agreed format to a centralised repository to be defined by Highways England.  |
|  |  **56.**   | **3rd Party Service Security** 56.1 The Supplier shall support Highways England to ensure that EUC devices are configured appropriately and can support the Customers approved Remote Access Security solution. 56.2 The WinTel Supplier shall support Highways England to ensure EUC devices are configured appropriately and can support the Firewall Management Service provided by the PSN Services IT Supplier. 56.3 The WinTel Supplier shall support Highways England to ensure EUC devices are configured appropriately and can support the Intrusion Prevention Service provided by the PSN Services IT Supplier and Hosting Services IT Supplier.  |
|  | **57.**  | **Data Encryption**  |

|  |  |  |
| --- | --- | --- |
|  |   | 57.1 The WinTel Supplier shall deploy, manage and maintain a Data Encryption Service for End User Devices to encrypt data either at rest on the End User Device or in transit over the remote access VPN to prevent data being disclosed or modified in an unauthorised way. 57.2 In providing the Data Encryption Service, the WinTel Supplier shall: 57.2.1 provide a service that can encrypt complete volumes at End Use Devices thus protecting all data at that End User Device from unauthorised disclosure; 57.2.2 provide reporting on End User Device encryption as requested by the Customer.  |
|  | **58.**  | **Investigation Support** 58.1 In providing the Investigation Support Service the WinTel Supplier shall: 58.1.1 comply with the requirements and standards set-out in the Customer’s forensic readiness policy; 58.1.2 maintain information sufficient to support investigations in progress and provide processes and tools to assist the Customer in preserving digital evidence. 58.1.3 support and assist with digital forensic investigation activities resulting from information leaking, fraud, disciplinary issues, inappropriate behaviour, accidents and negligence, commercial disputes and identity theft. 58.1.4 gather and provide information to support investigation activities; 58.1.5 ensure that such services can be carried out in such a manner as to minimise the impact to the Services – for the avoidance of doubt the Service Levels shall continue to apply during the course of any investigation activities; 58.1.6 hold evidence that can be reasonably provided for the Contract Period or as directed by the Customer of full audit records of investigation activities, securely and confidentially, and produce these on request to the Customer. 58.2 The WinTel Supplier shall support the Customer in the delivery of Information Security Audits.  |
|  |  **59.**  | **Security Monitoring and Alerting**  |

|  |  |
| --- | --- |
|  | 59.1 The WinTel Supplier shall provide a Security Monitoring and Alerting Service to supply management information on End User Device usage to inform the Customers risk position. 59.2 In providing the Security Monitoring and Alerting Service the WinTel Supplier shall: 59.2.1 monitor End User Device activities and security controls for security events, triage these events and alert appropriate events for the attention of the Customer; 59.2.2 perform remediation on low significance events found on End User Devices and log the activities for reporting; 59.2.3 escalate alerts of higher significance at given thresholds into the Customer’s security function; 59.2.4 provide alerting through open, non-proprietary standards; 59.2.5 provide End User Device log information to the Customer’s security function on request; 59.2.6 control End User Device access to assure the integrity of security log information; 59.2.7 provide reporting of monitoring and alert statistics and remediation; 59.2.8 provide reporting of performance and operational statistics to demonstrate and assure the correct operation of the controls on End User Devices; 59.2.9 provide evidence of the audit log repository and controls to protect the log information on End User Devices; 59.2.10implement monitoring that provides a real-time view of the operational status of security controls and events on End User Devices.  For all the above scope it is stated within the context of the provision of EUC services to the buyer, not any wider services. So, for example any DR requirement relates to the provision of EUC services, not the Buyer’s wider services.  For any stated scope it is assumed that the solution is technically feasible to implement by the provided tools or in line with the stated policy. If a policy defines something is not technically feasible to implement with the available tools, then this would be subject to discussion and impact with the Buyer.  It is assumed that the existing documentation set will be utilised and uplifted where required.   |

|  |  |
| --- | --- |
|  | It is assumed that this EUC Service is for the provision of a support team and all required HW and SW will be provided by the buyer. The only stated exclusion being the personnel’s own supplied Supplier local PC.   |
| **Additional services:**  | None  |
| **Location:**  | The Services will be delivered to Highways England in Leeds and where required, other Netcompany UK offices.  |
| **Quality standards:**  | The quality standards required for this Call-Off Contract are the Supplier will have in place and will operate in line to its defined Quality Framework. Such Framework will be based on the standards supported by ISO9001  |
| **Technical standards:**  | The technical standards required for this Call-Off Contract the Supplier is ISO9001 certified and all work will be carried out in accordance with such standards  |
| **Service level agreement:**  | The service level and availability criteria required for this Call-Off Contract are outlined in detail in section G-Cloud Services Required.  |
| **Onboarding:**  | The Supplier shall onboard initial resources by 05/11/18 to support the required shadowing and reverse shadowing activities prior to full transition of services.  |
| **Offboarding:**  | The services outlined within this Call-Off Contract shall be transitioned inhouse to Highways England at the end of the contract, subject to Highways England readiness. The offboarding plan for this Call-Off Contact will be agreed with Highways England.  |
| **Collaboration agreement:**  | N/A   |
| **Limit on** **Parties’ liability:**  | The annual total liability of either Party for all Property defaults will not exceed £1mn The annual total liability for Buyer Data defaults will not exceed 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). The annual total liability for all other defaults will not exceed the greater of 100% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater).   |
| **Insurance:**  | The insurance(s) required will be:  [a minimum insurance period of [6 years] following the expiration or Ending of this Call-Off Contract]  [professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law)]  |
|  |  [employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law]   |
| **Force majeure:**  | A Party may End this Call-Off Contract if the Other Party is affected by a Force Majeure Event that lasts for more than [enter text] consecutive days.  |
| **Audit:**  | The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-Off Contract to enable the Buyer to carry out audits. [Enter text]. [List the required audit provisions from clauses 7.3 to 7.12 of the Framework Agreement.]   |
| **Buyer’s responsibilities:**  | The Buyer is responsible for the following:  * The procurement and supply of any hardware and software required by the Supplier in the provision of the EUC Wintel Service
* Granting of access to required Highways England sites and locations
* Granting of access to required Highways England local computer rooms
* Granting of permissions to required systems, e.g. ServiceNow for the Supplier’s personnel to deliver the specified services
* Access to Highways England network via VPN to connect to the specified services

   |
| **Buyer’s equipment:**  | The Buyer’s equipment to be used with this Call-Off Contract includes:  * End User Devices (EUD) for the supply of the EUC Wintel Service
* Test EUD devices required by the Supplier
* Server infrastructure required within the SCC Sentinel or the Microsoft Azure platform to enable the Supplier to deliver the specified services.

   |

# Supplier’s information

|  |  |
| --- | --- |
| **Subcontractors or partners:**  | The following is a list of the Supplier’s Subcontractors or Partners [enter text]. [Include details of any Subcontractors to be used to deliver the Services.]  |

# Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

|  |  |
| --- | --- |
| **Payment method:**  | The payment method for this Call-Off Contract is a Service Charge  |
| **Payment profile:**  | The payment profile for this Call-Off Contract is monthly. [Many suppliers offer payment options, state here which method of payment and profile has been agreed. Buyers don’t have to agree to pay in advance.]  |
| **Invoice details:**  | The Supplier will issue electronic invoices monthly. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.  |
| **Who and where to send invoices to:**  | Invoices will be sent to [enter text].  |
| **Invoice information required** – for example purchase order, project reference:  | All invoices must include the Purchase Order number  |
| **Invoice frequency:**  | Invoice will be sent to the Buyer [enter text].  |
| **Call-Off Contract value:**  | The total value of this Call-Off Contract is £1,944,556  |
| **Call-Off Contract charges:**  | The breakdown of the Charges is based on a monthly Service charge and applicable charging for the additional services  |

# Additional buyer terms

|  |  |
| --- | --- |
| **Performance of the service and deliverables:**  | This Call-Off Contract will include the following implementation plan, exit and offboarding plans and milestones: * Contract Start: 5th November 2018
* Service Transition and go live: 17th December 2018
 |
|  | ●   | End of Service: 5th November 2020  |
| **Guarantee:**  | N/A  |  |
| **Warranties, representations:**  | N/A  |  |
| **Supplemental requirements in addition to the CallOff terms:**  | N/A  |  |
| **Alternative clauses:**  | N/A  |  |
| **Buyer specific** **amendments** **to/refinements of the Call-Off Contract terms:**  | Within the scope of the Call-Off Contract, the Supplier will [enter text]. [Delete if not relevant.]  |
| **Public Services Network (PSN):**  | The Public Services Network (PSN) is the Government’s secure network. If the G-Cloud Services are to be delivered over PSN this should be detailed here:  |
|  |  • The Supplier shall utilise Highways England equipment and connection to the PSN to deliver the specified services  |
| **Personal Data and Data Subjects:**  | Will Schedule 7 – Processing, Personal Data and Data Subjects be used Y/N [Delete as appropriate]  |

# 1. Formation of contract

1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.

1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.

1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.

1.4 In cases of any ambiguity or conflict the terms and conditions of the Call-Off Contract and Order Form will supersede those of the Supplier Terms and Conditions.

# 2. Background to the agreement

1. The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.10.
2. The Buyer provided an Order Form for Services to the Supplier.

|  |  |  |
| --- | --- | --- |
| **Signed:**  | Supplier  | Buyer  |
| **Name:**  | *Redacted*  |  *Redacted* |
| **Title:**  | CEO, UK & Vietnam  |  Group Procurement Manager |
| **Signature:**  | *Redacted*  | *Redacted*  |
| **Date:**  | 5th November 2018  | 06/11/18 |

**Schedule 1 - Services**

Digital Marketplace Service ID Number: 322803416669880

# Schedule 2 - Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the

Supplier’s Digital Marketplace pricing document) can’t be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will include:

# Wintel Service

* Year 1: £79,639.80 per month
* Year 2: £53,093.20 per month
* Total: £1,592,796

For any requested renewal beyond the initial term as a minimum inflation rate increases will apply to the continued charging.

**Part B - Terms and conditions**

# 1. Call-Off Contract start date and length

1.1 The Supplier must start providing the Services on the date specified in the Order Form.

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start Date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, as long as this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

# 2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:

* 4.1 (Warranties and representations)
* 4.2 to 4.7 (Liability)  4.11 to 4.12 (IR35)  5.2 to 5.3 (Force majeure)  5.6 (Continuing rights)  5.7 to 5.9 (Change of control)

5.10 (Fraud)  5.11 (Notice of fraud)  7.1 to 7.2 (Transparency)  8.3 (Order of precedence)  8.4 (Relationship)  8.7 to 8.9 (Entire agreement)  8.10 (Law and jurisdiction)  8.11 to 8.12 (Legislative change)  8.13 to 8.17 (Bribery and corruption)  8.18 to 8.27 (Freedom of Information Act)  8.28 to 8.29 (Promoting tax compliance)  8.30 to 8.31 (Official Secrets Act)  8.32 to 8.35 (Transfer and subcontracting)  8.38 to 8.41 (Complaints handling and resolution)  8.49 to 8.51 (Publicity and branding

* 8.42 to 8.48 (Conflicts of interest and ethical walls)  8.52 to 8.54 (Equality and diversity)  8.66 to 8.67 (Severability)  8.68 to 8.82 (Managing disputes)  8.83 to 8.91 (Confidentiality)
* 8.92 to 8.93 (Waiver and cumulative remedies)
* paragraphs 1 to 10 of the Framework Agreement glossary and interpretations  any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

* a reference to the ‘Framework Agreement’ will be a reference to the ‘Call-Off Contract’  a reference to ‘CCS’ will be a reference to ‘the Buyer’
* a reference to the ‘Parties’ and a ‘Party’ will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract
	1. The Framework Agreement incorporated clauses will be referred to as ‘incorporated Framework clause XX’, where ‘XX’ is the Framework Agreement clause number.
	2. When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

# 3. Supply of services

3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier’s Application.

3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer’s acceptance criteria, as defined in the Order Form.

# 4. Supplier staff

4.1 The Supplier Staff must:

* be appropriately experienced, qualified and trained to supply the Services  apply all due skill, care and diligence in faithfully performing those duties
* obey all lawful instructions and reasonable directions of the Buyer and provide the

Services to the reasonable satisfaction of the Buyer  respond to any enquiries about the Services as soon as reasonably possible  complete any necessary Supplier Staff vetting as specified by the Buyer

* 1. The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.
	2. The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
	3. The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier’s engagement under the Call-Off Contract is Inside or Outside IR35.
	4. The Buyer may End this Call-Off Contract for Material Breach if the Supplier is delivering the Services Inside IR35.
	5. The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start Date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.
	6. If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.
	7. If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

# 5. Due diligence

5.1 Both Parties agree that when entering into a Call-Off Contract they:

have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party

* are confident that they can fulfil their obligations according to the Call-Off Contract terms
* have raised all due diligence questions before signing the Call-Off Contract  have entered into the Call-Off Contract relying on its own due diligence

# 6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their service descriptions.

6.2 The Supplier’s business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer’s own plans.

# 7. Payment, VAT and Call-Off Contract charges

7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier’s delivery of the Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract, it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate rate.

7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer’s failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there’s an invoice dispute, the Buyer must pay the undisputed amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature of G-Cloud Services it isn’t possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer’s volumes indicated in the Order Form are indicative only.

# 8. Recovery of sums due and right of set-off

8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

# 9. Insurance

9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

9.2 The Supplier will ensure that:

* during this Call-Off Contract, Subcontractors hold third-party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000
* the third-party public and products liability insurance contains an ‘indemnity to principals’ clause for the Buyer’s benefit
* all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

all agents and professional consultants involved in the Services hold employers’ liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

* 1. If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.
	2. If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:
* a broker's verification of insurance  receipts for the insurance premium
* evidence of payment of the latest premiums due

9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

* take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers
* promptly notify the insurers in writing of any relevant material fact under any insurances
* hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

* 1. The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.
	2. The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.
	3. The Supplier will be liable for the payment of any:
* premiums, which it will pay promptly
* excess or deductibles and will not be entitled to recover this from the Buyer

# 10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection

Legislation or under incorporated Framework Agreement clauses 8.83 to 8.91. The

indemnity doesn’t apply to the extent that the Supplier breach is due to a Buyer’s instruction.

# 11. Intellectual Property Rights

11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its licensors.

11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royaltyfree licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer’s ordinary business activities.

11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs, so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer’s right to publish the IPR as open source.

11.4 The Supplier must promptly inform the Buyer if it can’t comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can’t obtain the grant of a licence acceptable to the Buyer.

11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party’s IPRs because of the:

* rights granted to the Buyer under this Call-Off Contract  Supplier’s performance of the Services  use by the Buyer of the Services

11.6 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

* modify the relevant part of the Services without reducing its functionality or performance
* substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer
* buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.7 Clause 11.5 will not apply if the IPR Claim is from:

* the use of data supplied by the Buyer which the Supplier isn’t required to verify under this Call-Off Contract

other material provided by the Buyer necessary for the Services

11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

# 12. Protection of information

12.1 The Supplier must:

* comply with the Buyer’s written instructions and this Call-Off Contract when Processing Buyer Personal Data  only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body
* take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

* providing the Buyer with full details of the complaint or request
* complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer’s instructions  providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)  providing the Buyer with any information requested by the Data Subject

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

# 13. Buyer data

The Supplier must not remove any proprietary notices in the Buyer Data.

13.1 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.

13.2 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

13.3 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier’s and Buyer’s security policy and all Buyer requirements in the Order Form.

13.4 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.

13.5 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

* the principles in the Security Policy Framework at https://www.gov.uk/government/publications/security-policy-framework and the Government Security Classification policy at

https://www.gov.uk/government/publications/government-security-classifications

* guidance issued by the Centre for Protection of National Infrastructure on Risk Management at https://www.cpni.gov.uk/content/adopt-risk-management-approach and Accreditation of Information Systems at https://www.cpni.gov.uk/protectionsensitive-information-and-assets
* the National Cyber Security Centre’s (NCSC) information risk management guidance, available at https://www.ncsc.gov.uk/guidance/risk-management-collection
* government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at

https://www.gov.uk/government/publications/technology-code-ofpractice/technology-code-of-practice

* the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance at https://www.ncsc.gov.uk/guidance/implementingcloud-security-principles
	1. The Buyer will specify any security requirements for this project in the Order Form.
	2. If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.
	3. The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

* 1. The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer’s Data.

# 14. Standards and quality

14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is available at

https://www.gov.uk/government/publications/technology-code-of-practice/technologycode-of-practice

14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN

Authority considers there is a risk to the PSN’s security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

# 15. Open source

15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.

15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

# 16. Security

16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer’s written approval of) a Security Management Plan and an Information Security

Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer’s security policy and protect all aspects and processes associated with the delivery of the Services.

16.2 The Supplier will use software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.

16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.

16.4 Responsibility for costs will be at the:

* Supplier’s expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided
* Buyer’s expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer’s control
	1. The Supplier will immediately notify CCS of any breach of security of CCS’s Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the CCS and Buyer Confidential Information however it may be recorded.
	2. Any system development by the Supplier should also comply with the government’s ‘10 Steps to Cyber Security’ guidance, available at https://www.ncsc.gov.uk/guidance/10steps-cyber-security
	3. If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start Date.

# 17. Guarantee

17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start Date:

* an executed Guarantee in the form at Schedule 5
* a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

# 18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days’ written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier’s obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

* Buyer’s right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided
* Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier’s avoidable costs or Losses
	1. Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.
	2. The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:
* a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied  any fraud

18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

* the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so
* an Insolvency Event of the other Party happens
* the other Party ceases or threatens to cease to carry on the whole or any material part of its business
	1. If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn’t pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.
	2. A Party who isn’t relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

# 19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the Ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date

(whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

* any rights, remedies or obligations accrued before its Ending or expiration
* the right of either Party to recover any amount outstanding at the time of Ending or expiry
* the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses 7 (Payment, VAT and Call-Off Contract charges); 8 (Recovery of sums due and right of set-off); 9 (Insurance); 10 (Confidentiality); 11 (Intellectual property rights); 12 (Protection of information); 13 (Buyer data);19 (Consequences of suspension, ending and expiry); 24 (Liability); incorporated Framework Agreement clauses: 4.2 to

4.7 (Liability); 8.42 to 8.48 (Conflicts of interest and ethical walls) and 8.92 to 8.93 (Waiver and cumulative remedies)

● any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

* return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
* return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
* stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer
* destroy all copies of the Buyer Data when they receive the Buyer’s written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law
* work with the Buyer on any ongoing work
* return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date
	1. Each Party will return all of the other Party’s Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.
	2. All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

# 20. Notices

20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.

|  |  |  |
| --- | --- | --- |
| **Manner of delivery**  | **Deemed time of delivery**  | **Proof of service**  |
| Email  | 9am on the first Working Day after sending  | Sent by PDF to the correct email address without getting an error message  |

20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

# 21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier’s own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start Date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier’s methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer’s own exit plan and strategy.

21.6 The Supplier acknowledges that the Buyer’s right to extend the Term beyond 24 months is subject to the Buyer’s own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier’s additional exit plan ensures that:

* the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer
* there will be no adverse impact on service continuity  there is no vendor lock-in to the Supplier’s Service at exit
* it enables the Buyer to meet its obligations under the Technology Code of Practice
	1. If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.
	2. The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:
* the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier
* the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer
* the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier
* the testing and assurance strategy for exported Buyer Data  if relevant, TUPE-related activity to comply with the TUPE regulations
* any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

# 22. Handover to replacement supplier

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

* data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier’s possession, power or control
* other information reasonably requested by the Buyer
	1. On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This

will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

* 1. This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

# 23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than the number of consecutive days set out in the Order Form, the other Party may End this Call-Off Contract with immediate effect by written notice.

# 24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.2 to 4.7, each Party's Yearly total liability for defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:

* Property: for all defaults resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form  Buyer Data: for all defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data caused by the Supplier's default will not exceed the amount in the Order Form
* Other defaults: for all other defaults, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form

# 25. Premises

25.1 If either Party uses the other Party’s premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer’s premises solely for the performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer’s premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer’s premises, the Supplier will:

* comply with any security requirements at the premises and not do anything to weaken the security of the premises
* comply with Buyer requirements for the conduct of personnel  comply with any health and safety measures implemented by the Buyer
* immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

# 26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

# 27. The Contracts (Rights of Third Parties) Act 1999

27.1 Except as specified in clause 29.8, a person who isn’t Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

# 28. Environmental requirements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

# 29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start Date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer’s request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

* the activities they perform
* age
* start date  place of work  notice period
* redundancy payment entitlement  salary, benefits and pension entitlements  employment status  identity of employer  working arrangements  outstanding liabilities  sickness absence
* copies of all relevant employment contracts and related documents
* all information required under regulation 11 of TUPE or as reasonably requested by the Buyer
	1. The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.
	2. In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.
	3. The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.
	4. The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:
* its failure to comply with the provisions of this clause
* any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer
	1. The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.
	2. For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause, but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

# 30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn’t have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

# 31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start Date.

31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:

* work proactively and in good faith with each of the Buyer’s contractors
* co-operate and share information with the Buyer’s contractors to enable the efficient operation of the Buyer’s ICT services and G-Cloud Services

# 32. Variation process

32.1 The Buyer can request in writing a change to this Call-Off Contract if it isn’t a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier’s supply chain.

32.3 If Either Party can’t agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this CallOff Contract by giving 30 days notice to the Supplier.

# 33. Data Protection Legislation (GDPR)

33.1 The Parties will comply with the Data Protection Legislation and agree that the Buyer is the Controller and the Supplier is the Processor. The only Processing the Supplier is authorised to do is listed at Schedule 7 unless Law requires otherwise (in which case the Supplier will promptly notify the Buyer of any additional Processing if permitted by Law).

33.2 The Supplier will assist the Buyer with the preparation of any Data Protection Impact Assessment required by the Data Protection Legislation before commencing any Processing (including provision of detailed information and assessments in relation to Processing operations, risks and measures) and must notify the Buyer immediately if it considers that the Buyer’s instructions infringe the Data Protection Legislation.

33.3 The Supplier must have in place Protective Measures, details of which shall be provided to the Buyer on request, to guard against a Data Loss Event, which take into account the nature of the data, the harm that might result, the state of technology and the cost of implementing the measures.

33.4 The Supplier will ensure that the Supplier Staff only process Personal Data in accordance with this Call-Off Contract and take all reasonable steps to ensure the reliability and integrity of Supplier staff with access to Personal Data, including by ensuring they:

i) are aware of and comply with the Supplier’s obligations under this Clause; ii) are subject to appropriate confidentiality undertakings with the Supplier

iii) are informed of the confidential nature of the Personal Data and don’t publish, disclose or divulge it to any third party unless directed by the Buyer or in accordance with this Call-Off Contract iv) are given training in the use, protection and handling of Personal Data.

33.5 The Supplier will not transfer Personal Data outside of the European Union unless the prior written consent of the Buyer has been obtained, which shall be dependent on such a transfer satisfying relevant Data Protection Legislation requirements.

33.6 The Supplier will delete or return Buyer’s Personal Data (including copies) if requested in writing by the Buyer at the End or Expiry of this Call-Off Contract, unless required to retain the Personal Data by Law.

33.7 The Supplier will notify the Buyer without undue delay if it receives any communication from a third party relating to the Parties’ obligations under the Data Protection Legislation, or it becomes aware of a Data Loss Event, and will provide the Buyer with full and ongoing assistance in relation to each Party’s obligations under the Data Protection Legislation, and

insofar as this is possible, in accordance with any timescales reasonably required by the Buyer

33.8 The Supplier will maintain complete and accurate records and information to demonstrate its compliance with this clause. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:

i) the Buyer determines that the Processing is not occasional; ii) the Buyer determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

iii) the Buyer determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

33.9 Before allowing any Sub-processor to Process any Personal Data related to this Call-Off Contract, the Supplier must:

* 1. notify the Buyer in writing of the proposed Sub-processor(s) and obtain its written consent;
	2. ensure that it has entered into a written agreement with the Subprocessor(s) which gives effect to obligations set out in this Clause 33 such that they apply to the Sub-processor(s); and iii. inform the Buyer of any additions to, or replacements of the notified Sub-processors and the Buyer shall either i) provide its written consent or ii) object.

33.10 The Buyer may at any time put forward a Variation request to amend this Call-Off Contract to ensure that it complies with any guidance issued by the Information Commissioner’s Office.

# Schedule 3 - Collaboration agreement

The Collaboration agreement is available at https://www.gov.uk/guidance/g-cloud-templates-andlegal-documents

# Schedule 4 - Alternative clauses

The Alternative clauses are available at https://www.gov.uk/guidance/g-cloud-templates-andlegal-documents

# Schedule 5 - Guarantee

The Guarantee is available at https://www.gov.uk/guidance/g-cloud-templates-and-legaldocuments

# Schedule 6 - Glossary and interpretations

In this Call-Off Contract the following expressions mean:

|  |  |
| --- | --- |
| **Additional Services**  | Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.  |
| **Admission Agreement**  | The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).  |
| **Application**  | The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).  |
| **Audit**  | An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).  |
| **Background IPRs**  | For each Party, IPRs: * owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes
* created by the Party independently of this Call-Off Contract, or

 For the Buyer, Crown Copyright which isn’t available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.  |
| **Buyer**  | The contracting authority ordering services as set out in the Order Form.  |
| **Buyer Data**  | All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.  |
| **Buyer Personal Data**  | The personal data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.  |

|  |  |
| --- | --- |
| **Buyer Representative**  | The representative appointed by the Buyer under this Call-Off Contract.  |
| **Buyer Software**  | Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.  |
| **Call-Off Contract**  | This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.  |
| **Charges**  | The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.  |
| **Collaboration Agreement**  | An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer’s Services and to ensure that the Buyer receives endto-end services across its IT estate.  |
| **Commercially Sensitive Information**  | Information, which the Buyer has been notified about by the Supplier in writing before the Start Date with full details of why the Information is deemed to be commercially sensitive.  |
| **Confidential Information**  | Data, personal data and any information, which may include (but isn’t limited to) any: * information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above
* other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
 |
| **Control**  | ‘Control’ as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.  |
| **Controller**  | Takes the meaning given in the Data Protection Legislation.  |
| **Crown**  | The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.  |

|  |  |
| --- | --- |
| **Data Loss Event** | Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed  |
| **Data Protection Impact Assessment**  | An assessment by the Controller of the impact of the envisaged processing by the Processor under this Call-Off Contract on the protection of Personal Data.  |
| **Data Protection Legislation**  |  Data Protection Legislation means:  i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time ii) the DPA 2018 to the extent that it relates to processing of personal data and privacy; iii) all applicable Law about the processing of personal data and privacy, including if applicable legally binding guidance and codes of practice issued by the Information Commissioner.  |
| **Data Subject**  | Takes the meaning given in the Data Protection Legislation.  |
| **Default**  | Default is any: * breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term)
* other default, negligence or negligent statement of the

Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract  Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.  |
| **Deliverable**  | The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.  |
| **Digital Marketplace**  | The government marketplace where Services are available for Buyers to buy. (https://www.digitalmarketplace.service.gov.uk/)  |
| **DPA 2018**  | Data Protection Act 2018.  |
| **Employment Regulations**  | The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) (‘TUPE’) which implements the Acquired Rights Directive.  |

|  |  |
| --- | --- |
| **End**  | Means to terminate; and Ended and Ending are construed accordingly.  |
| **Environmental Information Regulations or EIR**  | The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department about the regulations.  |
| **Equipment**  | The Supplier’s hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.  |
| **ESI Reference Number**  | The 14 digit ESI reference number from the summary of outcome screen of the ESI tool.  |
| **Employment Status** **Indicator test tool or ESI tool**  | The HMRC Employment Status Indicator test tool. The most upto-date version must be used. At the time of drafting the tool may be found here: http://tools.hmrc.gov.uk/esi  |
| **Expiry Date**  | The expiry date of this Call-Off Contract in the Order Form.  |
| **Force Majeure**  | A Force Majeure event means anything affecting either Party's performance of their obligations arising from any: * acts, events or omissions beyond the reasonable control of the affected Party
* riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare
* acts of government, local government or Regulatory

Bodies  fire, flood or disaster and any failure or shortage of power or fuel * industrial dispute affecting a third party for which a substitute third party isn’t reasonably available

 The following do not constitute a Force Majeure event: * any industrial dispute about the Supplier, its staff, or failure in the Supplier’s (or a Subcontractor's) supply chain
* any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure
* the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into
 |

|  |  |
| --- | --- |
|  |  any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans  |
| **Former Supplier**  | A supplier supplying services to the Buyer before the Start Date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).  |
| **Framework Agreement**  | The clauses of framework agreement RM1557.10 together with the Framework Schedules.  |
| **Fraud**  | Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this CallOff Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.  |
| **Freedom of Information Act or FOIA**  | The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant Government department in relation to the legislation.  |
| **G-Cloud Services**  | The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.  |
| **GDPR**  | The General Data Protection Regulation (Regulation (EU) 2016/679).  |
| **Good Industry Practice**  | Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.  |
| **Guarantee**  | The guarantee described in Schedule 5.  |
| **Guidance**  | Any current UK Government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK Government guidance and the Crown Commercial Service guidance, current UK Government guidance will take precedence.  |

|  |  |
| --- | --- |
| **Indicative Test**  | ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.  |
| **Information**  | Has the meaning given under section 84 of the Freedom of Information Act 2000.  |
| **Information Security Management System**  | The information security management system and process developed by the Supplier in accordance with clause 16.1.  |
| **Inside IR35**  | Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.  |
| **Insolvency Event**  | Can be: * a voluntary arrangement  a winding-up petition
* the appointment of a receiver or administrator
* an unresolved statutory demand  a Schedule A1 moratorium.
 |
| **Intellectual Property Rights or IPR**  | Intellectual Property Rights are: * copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential

Information  applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction * all other rights having equivalent or similar effect in any country or jurisdiction
 |
| **Intermediary**  | For the purposes of the IR35 rules an intermediary can be:  the supplier's own limited company  a service or a personal service company  a partnership  It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).  |
| **IPR Claim**  | A claim as set out in clause 11.5.  |
| **IR35**  | IR35 is also known as ‘Intermediaries legislation’. It’s a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.  |

|  |  |
| --- | --- |
| **IR35 Assessment**  | Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.  |
| **Know-How**  | All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding knowhow already in the Supplier’s or CCS’s possession before the Start Date.  |
| **Law**  | Any applicable Act of Parliament, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, exercise of the royal prerogative, enforceable community right within the meaning of Section 2 of the European Communities Act 1972, judgment of a relevant court of law, or directives or requirements of any Regulatory Body.  |
| **LED**  | Law Enforcement Directive (EU) 2016/680.  |
| **Loss**  | All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.  |
| **Lot**  | Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.  |
| **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.  |
| **Management Charge**  | The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.  |
| **Management Information**  | The management information specified in Framework Agreement section 6 (What you report to CCS).  |
| **Material Breach**  | Those breaches which have been expressly set out as a material breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.  |

|  |  |
| --- | --- |
| **Ministry of Justice Code**  | The Ministry of Justice’s Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.  |
| **New Fair Deal**  | The revised Fair Deal position in the HM Treasury guidance: “Fair Deal for staff pensions: staff transfer from central government” issued in October 2013 as amended.  |
| **Order**  | An order for G-Cloud Services placed by a Contracting Body with the Supplier in accordance with the Ordering Processes.  |
| **Order Form**  | The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.  |
| **Ordered G-Cloud Services**  | G-Cloud Services which are the subject of an Order by the Buyer.  |
| **Outside IR35**  | Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.  |
| **Party**  | The Buyer or the Supplier and ‘Parties’ will be interpreted accordingly.  |
| **Personal Data**  | Takes the meaning given in the Data Protection Legislation.  |
| **Personal Data Breach**  | Takes the meaning given in the Data Protection Legislation.  |
| **Processing**  | Takes the meaning given in the Data Protection Legislation but, for the purposes of this Call-Off Contract, it will include both manual and automatic Processing. ‘Process’ and ‘processed’ will be interpreted accordingly.  |
| **Processor**  | Takes the meaning given in the Data Protection Legislation.  |
| **Prohibited Act**  | To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: * induce that person to perform improperly a relevant function or activity
* reward that person for improper performance of a relevant function or activity
* commit any offence:
	+ under the Bribery Act 2010
	+ under legislation creating offences concerning Fraud
	+ at common Law concerning Fraud
 |

|  |  |
| --- | --- |
|  |  committing or attempting or conspiring to commit Fraud  |
| **Project Specific IPRs**  | Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier’s Background IPRs.  |
| **Property**  | Assets and property including technical infrastructure, IPRs and equipment.  |
| **Protective Measures**  | Appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.  |
| **PSN or Public Services Network**  | The Public Services Network (PSN) is the Government’s highperformance network which helps public sector organisations work together, reduce duplication and share resources.  |
| **Regulatory Body or Bodies**  | Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.  |
| **Relevant Person**  | Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.  |
| **Relevant Transfer**  | A transfer of employment to which the Employment Regulations applies.  |
| **Replacement Services**  | Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the Services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.  |
| **Replacement Supplier**  | Any third party service provider of Replacement Services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).  |
| **Services**  | The services ordered by the Buyer as set out in the Order Form.  |

|  |  |
| --- | --- |
| **Service Data**  | Data that is owned or managed by the Buyer and used for the GCloud Services, including backup data.  |
| **Service Definition(s)**  | The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn’t limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.  |
| **Service Description**  | The description of the Supplier service offering as published on the Digital Marketplace.  |
| **Service Personal Data**  | The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.  |
| **Spend Controls**  | The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spendcontrols-check-if-you-need-approval-to-spend-money-on-aservice  |
| **Start Date**  | The start date of this Call-Off Contract as set out in the Order Form.  |
| **Subcontract**  | Any contract or agreement or proposed agreement between the Supplier and a Subcontractor in which the Subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.  |
| **Subcontractor**  | Any third party engaged by the Supplier under a Subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.  |
| **Subprocessor**  | Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.  |
| **Supplier Representative**  | The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.  |
| **Supplier Staff**  | All persons employed by the Supplier together with the Supplier’s servants, agents, suppliers and Subcontractors used in the performance of its obligations under this Call-Off Contract.  |
| **Supplier Terms**  | The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier’s Application.  |
| **Term**  | The term of this Call-Off Contract as set out in the Order Form.  |
| **Variation**  | This has the meaning given to it in clause 32 (Variation process).  |
| **Working Days**  | Any day other than a Saturday, Sunday or public holiday in England and Wales.  |
| **Year**  | A contract year.  |

# Schedule 7 - Processing, Personal Data and Data Subjects

**Subject matter of the processing:**

 The Subject Matter is all user account information required to managed Active Directory and Exchange services

**Duration of the processing:**

The processing will take place for the duration of the contract, and will end when the contract terminates.

**Nature and purposes of the Processing:**

The data to be included is names and user IDs for all users on the Highways England estate, as required to effectively manage user accounts and access to services in the Highways England IT estate. All access to this data will be made by staff with suitable Security Clearance (BPSS, and in the case of admin accounts either SC clearance or evidence of working towards SC clearance)

**Type of Personal Data:**

Name and User ID, email address.

**Categories of Data Subject:**

Staff (including volunteers, agents and temporary workers), and suppliers with Highways England accounts.

**Plan for return or destruction of the data once the Processing is complete UNLESS requirement under union or member state law to preserve that type of data:**

The data will all be accessed on the Highways England estate, so there is no specific need to return or destroy the data. Data from users who leave Highways England will be deleted in line with Highways England User Account policies.