Department
for Environment
Food & Rural Affairs

Future End User Services Procurement Project (FEUSPP)

Ref: Project_30635

Volume: 4 (Commercial Compliance Tender Templates)
Document: 2 (Requirements Compliance Matrix)

Date: August 2024
Version: 2.0

ITT VOLUME 4_ DOCUMENT_2 REQUIREMENTS COMPLIANCE MATRIX

The purpose of this document is to enable the Bidders to submit their compliance response to the FEUSPP Buyer's Requirements.

Summary Instructions

Bidders are required to note the following:

1) The Buyer Requirements ID, Operational Area, Service Function, Requirement description and MOSCOW match the ITT Volume 2_Document_1 (Requirements).

2) The MOSCOW identifies the Requirement priortisation, mainly MUST and SHOULD.

3) Bidder Compliance Response : For each Requirement please enter whether you "Fully Compliant", "Partially Compliant" or "Non-Compliant" to confirm the extent to which you satisfy the Requirement.

4) Compliance Statement: For each Requirement please provide an explanation of the Compliance Response, limited to 100 words.

5) ITT Volume 1_Document 2_Evaluation Methodology provides the Buyer's Mandatory Requirements (MUSTs) scoring criteria including the quality scoring criteria for SHOULDs.

BUYER REQUIREMENTS					BIDDER COMPLIANCE RESPONSE	
ID	Operational Area	Service Function	Requirement	MoSCoW	Fully Compliant Partially Compliant Non-Compliant	COMPLIANCE STATEMENT [MAX 100 Words]
SSM.001	Service Management	**Supplier Management**	The Supplier must operate Supplier Management in accordance with the Buyer's Supplier Management Policy - "SMSI-071-001-022 Defra Supplier Management Policy" and Supplier Management Process - "SMSI-071-002-022 Defra Supplier Management Process".	**Must**		[redacted]
SSM.002	Service Management	**Supplier Management**	The Supplier must develop and execute a plan for Value Release initiatives, identifying activities that unlock additional improvements and opportunities to deliver value to the Buyer and its stakeholders, refer to: Buyer's Supplier Management Policy - "SMSI-071-001-022 Defra Supplier Management Policy" and Supplier Management Process - "SMSI-071-002-022 Defra Supplier Management Process".	**Must**		
SSM.003	Service Management	**Supplier Management**	The Supplier must work with the Buyer to develop and maintain an Account Management Plan incorporating all contracts held with the Buyer, refer to: Buyer's Supplier Management Policy - "SMSI-071-001-022 Defra Supplier Management Policy" and Supplier Management Process - "SMSI-071-002-022 Defra Supplier Management Process".	**Must**		
SSM.004	Service Management	**Supplier Management**	The Supplier must operate with other Suppliers contracted by the Buyer, in accordance with the "Collaboration Agreement".	**Must**		
SSM.005	Service Management	**Supplier Management**	Suppliers must participate in all of the following Buyer collaboration activities, in line with Call Off Schedule 7 (Governance): Participate and show attendance at all Supplier all hands calls. Utilise the Supplier Connect portal for collaborative working and keeping abreast of the Buyer Supplier related news. Participate and show attendance at bi-annual cross Supplier strategy away days.	**Must**		
SSM.006	Service Management	**Supplier Management**	The Supplier must contribute to service and product Continuous Improvement plans - refer to Call Off Schedule 17 (Continuous Improvement) - and product roadmaps.	**Must**		
SSM.007	Service Management	**Supplier Management**	The Supplier must report 'open book' data through the supply chain to evidence value for money and appropriate use of public funds, in line with the Buyer's Supplier Management Policy - "SMSI-071-001-022 Defra Supplier Management Policy" and Supplier Management Process - "SMSI-071-002-022 Defra Supplier Management Process".	**Must**		
SSM.008	Service Management	**Supplier Management**	The Supplier must participate in the Buyer's Supplier Relationship Management (SRM) meeting(s) and work to Key Performance Indicators (KPIs), participate in governance groups, incentivises innovation goals as descr bed in Call Off Schedule 7 (Governance).	**Must**		
SSM.009	Service Management	**Supplier Management**	Suppliers must participate and show attendance at Supplier Relationship Management (SRM) /Service Management Boards (SMB) meetings and a Quarterly Business Review (QBR) as descr bed in Call Off Schedule 7 (Governance). At a minimum the Supplier must have the following personnel in attendance: Account Manager, Service Delivery Executive/Manager, Operational Delivery Manager, Service Delivery Representatives, Head of Security, Data Manager	**Must**		
SSM.010	Service Management	**Supplier Management**	Suppliers must provide Supplier Management Reporting at all Supplier Relationship Management (SRM) /Service Management Boards (SMB) and a Quarterly Business Review (QBR). As a minimum, Supplier Management Reporting must include (but is not limited to): Contractual Report Compliance, Service performance Report, High Profile Incidents and Events, Service Levels Performance Overview, Business Impact, Priority Level 1, 2, 3, 4 MI, Incident Management Trend Analysis, Service Requests, Structured Cabling Faults, Service Credits, Capacity Management, Availability Management, Smart Lockers, Change Management, Actual Experience, Virtual Tech Bar Statistics, Actual Experience Improvement Investigations, Operational Delivery, Operational Service Improvements, Service Heatmaps, Minor works/Investment Recomendations, Executive Summary, Service Risks & Issues, Escalations and recommendations to other Boards.	**Must**		
SSM.011	Service Management	**Supplier Management**	The Service Management Board must be responsible for the management of the operational delivery of the technical aspects of the Services within the bounds of the Contract. The Supplier must: (a) Consider issues relating to the operational aspects of the Services including reviewing the Performance Monitoring Reports: (b) Confirming the submission of reports as outlined within the Call Off Schedule 3 (Service Levels, Service Credits and Performance Monitoring) and agree Service Levels attainment, Service Credits and relevant Performance Monitoring Reports; (c) At least annually, review the accuracy and completeness of Staffing Information, Asset and IPR reports provided pursuant to the Call Off Schedule 3 (Service Levels, Service Credits and Performance Monitoring); (d) Review operational delivery risks and issues and update the appropriate risks and issues registers; (e) Identify areas for improvements to Services;	**Must**		
SSM.012	Service Management	**Supplier Management**	The Supplier must operate and comply to all onboarding aspects of the Buyer's on-boarding process - "SMSI-01-321-002 On-boarding and Off-boarding process and approach".	**Must**		

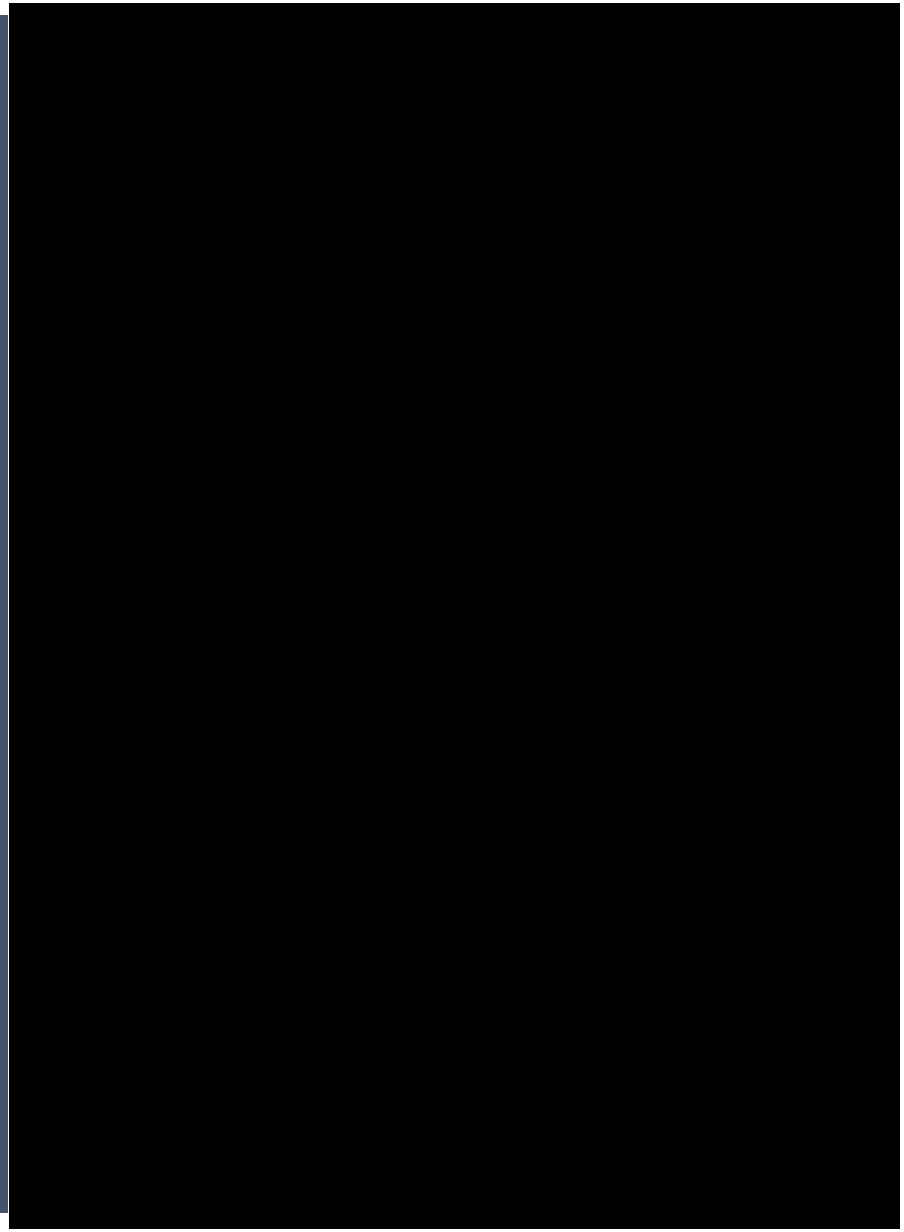
BUYER REQUIREMENTS					BIDDER COMPLIANCE RESPONSE	
ID	Operational Area	Service Function	Requirement	MoSCoW	Fully Compliant Partially Compliant Non-Compliant	COMPLIANCE STATEMENT [MAX 100 Words]
SMR.001	Service Management and Service Integration	**Service Management**	The Supplier must provide services that conform and adhere to the principles recognised within industry service management standards and as adopted by the Buyer. The Buyer is currently following the ITIL V3 framework but has an aspiration to migrate to ITIL V4. The Supplier shall have relevant staff trained at the ITIL V4 Foundation level to support the Buyers aspiration.	**Must**		[redacted]
SMR.002	Service Management and Service Integration	**Service Management**	The Supplier must operate within the Buyer's service management processes and service desk provision and as part of the Buyer's role as the Service Integrator within a Service Integration and Management (SIAM) model.	**Must**		
SMR.003	Service Management and Service Integration	**Service Management**	The Supplier must operate and conform with the principles set out in the Buyer's Service Run Manual (ref: SMSI-01-363-001)	**Must**		
SMR.004	Service Management and Service Integration	**Service Management**	The Supplier must work within the Buyer's IT Service Management toolset, for operational processes and service performance reporting against SLAs.	**Must**		
SMR.005	Service Management and Service Integration	**Service Management**	The Supplier shall ensure that its functional teams within the overall delivery of the Service communicate in a timely and effective way to ensure that responsibilities are clear and supported across the Suppliers whole delivery team.	**Must**		
SMR.006	Service Management and Service Integration	**Service Management**	The Supplier must work collaboratively with other Buyer suppliers, for example: third party suppliers; integral organisational units e.g. Arms' Length Bodies, to deliver seamless operational services.	**Must**		
SMR.007	Service Management and Service Integration	**Service Management**	The Supplier must commit to adopting a 'fix first, find fault later' approach when dealing with Service Issues and Incidents. This includes but not limited to, the following activities: (a)prompt notification of Service Issues and Incidents to the Buyer and, where appropriate, notification to other Buyer Suppliers; (b)prioritise achieving solutions to Service Issues and Incidents over seeking to blame any other parties;	**Must**		
SMR.008	Service Management and Service Integration	**Service Management**	The supplier staffing model must include but not be restricted to individual skills and experience of ITIL qualification certified as a minimum. 1) The Buyer is currently following the ITIL V3 framework but has an aspiration to migrate to ITIL V4. The Supplier shall have	**Must**		
SMR.009	Service Management and Service Integration	**Service Desk**	The Supplier must use Buyer's ITSM toolset, currently this is ServiceNow for operational processes and service performance reporting against SLAs, in the management and execution of its activities for the Service Desk End User provision.	**Must**		
SMR.010	Service Management and Service Integration	**Service Desk**	The Supplier must provide a 24 hours a day, 365 days per year (366 days in a leap year) English speaking Service Desk provision for the reporting, monitoring, management and communication related to Incidents, Problems, Service Requests, complaints and enquiries.	**Must**		
SMR.011	Service Management and Service Integration	**Service Desk**	The Supplier must be a key partner in supporting the Buyer's drive to shift-left through maximising First Contact Resolution (FCR) opportunities and self-help provision that will be aligned to contractual requirements to support and incentivise the sharing of knowledge utilised to achieve increases within FCR % over the term. This includes First Contact Resolution within the agreed Service Levels, before assigning the requirement of the ticket as set out by the Buyer's Service Management Process & Procedures. The First Contact Resolution (FCR) should include as a minimum: - Tips, quick-fixes and other methods to resolve Incidents;	**Must**		
SMR.012	Service Management and Service Integration	**Service Desk**	The Supplier must provide Telephony MI that is a true indication of compliance and call metrics as detailed in the Call Off Schedule 3 (Service Levels, Service Credits and Performance Monitoring)	**Must**		
SMR.013	Service Management and Service Integration	**Service Desk**	The Supplier must provide access to their Service Desk Policies, Procedures and Work Instructions, available to the Buyer and if required, to the Buyer's partner Suppliers.	**Must**		
SMR.014	Service Management and Service Integration	**Service Desk**	The Supplier must be able to cater for different types of users; including but not limited to: Standard Office Users Standard Field Users Assistive Technology Users VIP Users	**Must**		
SMR.015	Service Management and Service Integration	**Service Desk**	The Supplier must submit requests via the Service Catalogue ITSM toolset, (currently this is ServiceNow) on behalf of customers when contacted to do so.	**Must**		
SMR.016	Service Management and Service Integration	**Service Desk**	The Supplier must manage customer queries relating to requests submitted through the Service Catalogue ITSM toolset, (currently this is ServiceNow) on behalf of customers when contacted to do so.	**Must**		

SMR.017	Service Management and Service Integration	**Service Desk**	The Supplier must adhere to the Buyer's Request Fulfilment process for prioritisation and escalation of VIP user Requests and/or Incident/Major Incident Requests. The Supplier must assign this request to the relevant VIP resolving team, as instructed by the Buyer.	**Must**
SMR.018	Service Management and Service Integration	**Service Desk**	The Supplier must provide dedicated Tech bar personnel in key Buyer offices where users can receive face-to-face support. Tech bar personnel operate within core Buyer hours (typically Monday- Friday 08:00 - 18:00) and must assist with incident resolution and request fulfilment, desk side support, over and above that provided by the Service Desk and 2nd line support functions.	**Must**
SMR.019	Service Management and Service Integration	**Incident Management**	The Supplier must operate Incident Management in accordance with the Buyer's Incident Management policy and Incident Management Process (SMSI-071-002-006)	**Must**
SMR.020	Service Management and Service Integration	**Incident Management**	The Supplier must ensure that all Incidents are managed and maintained during the Incident resolution lifecycle. For this, the Supplier shall:	**Must**
SMR.021	Service Management and Service Integration	**Incident Management**	Service Desk supplier will actively manage tickets throughout the incident lifecycle in accordance to Buyer processes to ensure expected SLAs are met. The Supplier shall liaise with other Buyer Suppliers and resolver groups to ensure this actively occurs and will escalate accordingly to the Buyer where there is non-adherence. The Supplier must ensure that all tickets raised are managed in accordance to the agreed service level. This applies to both user and supplier raised tickets.	**Must**
SMR.022	Service Management and Service Integration	**Incident Management**	The Supplier must be a key partner and work collaboratively with the Buyer supporting its drive to shift-left through maximising first-time fix and sharing the Service Desk's knowledge within the Buyer's end users.	**Must**
SMR.023	Service Management and Service Integration	**Incident Management**	During times of national emergency the Supplier must provide provisions to operate an extended or expanded service where requested and deemed necessary an instructed to do so by the Buyer authorised representative(s).	**Must**
SMR.024	Service Management and Service Integration	**Incident Management**	The Buyer reserves the right to determine an Incident Resolution Priority for any Incident different to that assigned by the Supplier in the first instance, and the Supplier must accept the Buyer mandated Incident Resolution Priority and ensure that all tickets raised must be managed in accordance with the agreed service level.	**Must**
SMR.025	Service Management and Service Integration	**Incident Management**	The Supplier must work with third parties to resolve the Incident and escalate any issues encountered whilst attempting to restore the normal service expectations impacted by an Incident. Where the Supplier is the resolver, they must act as the primary to co-ordinate activities with any related Buyer Suppliers or resolver teams.	**Must**
SMR.026	Service Management and Service Integration	**Major Incident Management**	The Supplier must participate in Major Incident Management as requested and directed by the Buyer on a 24/7, 365 days per year (366 days in a leap year) basis in accordance with the Major Incident Management sections of the Buyer's Incident Management Policy (SMSI-071-001-006) and Incident Management Process (SMSI-071-002-006).	**Must**
SMR.027	Service Management and Service Integration	**Major Incident Management**	The Supplier must classify all Priority Level 1 Incidents as 'Major Incidents' as set out in the Buyers Incident Priority matrix.	**Must**
SMR.028	Service Management and Service Integration	**Major Incident Management**	The Supplier must ensure that all Major Incident Management tickets raised are updated in accordance within the SLA's as outlined within the Call Off Schedule 3 (Service Levels, Service Credits and Performance Monitoring).	**Must**
SMR.029	Service Management and Service Integration	**Problem Management**	The Supplier must operate Problem Management in accordance with the Buyer's Problem Management Policy - "SMSI-071-001-011 Defra Problem Management Policy", Problem Management Process - "SMSI-071-001-011 Defra Problem Management Policy".	**Must**
SMR.030	Service Management and Service Integration	**Problem Management**	The Supplier must proactively conduct Problem Management where trend analysis has identified recurring and repeat Incidents, with a view of implementing remediation in order to remove future reoccurrence of Incidents.	**Must**
SMR.031	Service Management and Service Integration	**Problem Management**	The Supplier must for each problem affecting the Services, provide comprehensive problem resolution activities and proposal(s) to the Service Desk Supplier for submission to the Buyer.	**Must**
SMR.032	Service Management and Service Integration	**Problem Management**	The Supplier must ensure Problems are documented to allow effective audit of Problem Management	**Must**
SMR.033	Service Management and Service Integration	**Problem Management**	The Supplier must implement the approved problem resolution pursuant to the Buyer's Change and Evaluation Management Policy - "SMSI-071-001-003 Defra Change and Evaluation Management Policy".	**Must**
SMR.034	Service Management and Service Integration	**Problem Management**	The Supplier must resolve problems to the satisfaction of the Buyer's Service Owner/Service Manager and update resolution details in the Buyer's IT Service Management system (ServiceNow), as per the SLA within the Call Off Schedule 3 (Service Levels, Service Credits and Performance Monitoring).	**Must**
SMR.035	Service Management and Service Integration	**Problem Management**	The Supplier must on the Buyer's request participate or provide input to, the Buyer's Problem Management regular governance forums where requested.	**Must**
SMR.036	Service Management and Service Integration	**Problem Management**	The Supplier must perform a root cause analysis in accordance with the Buyer's Problem Management process - "SMSI-071-002-011 Defra Problem Management Process", and within the agreed Service Levels	**Must**
SMR.037	Service Management and Service Integration	**Problem Management**	The Supplier must work collaboratively with the Buyer's third party Suppliers for the management and handling of Problems.	**Must**
SMR.038	Service Management and Service Integration	**Problem Management**	The Supplier must provide early engagement (in advance of new services going live) for new services to understand how Problem Management will or will not be executed and ensure all key info (information required in the Problem Management tab of the Service Design Package) collated.	**Must**

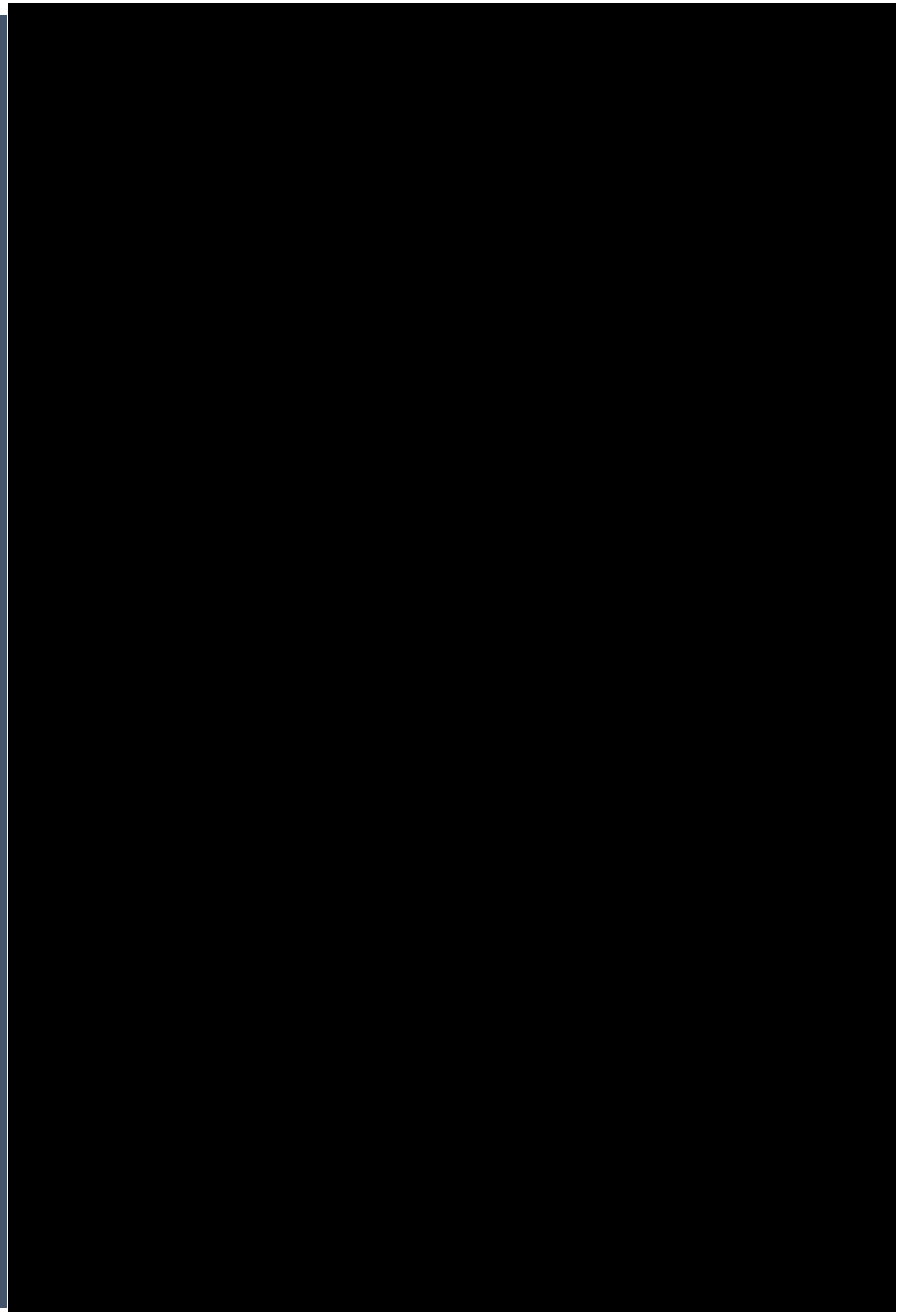
[redacted]

SMR.039	Service Management and Service Integration	**Problem Management**	The Supplier must provide timed, targeted reporting as specified in Service Levels where relevant, otherwise in accordance with business requirements, to allow the effectiveness of Problem Management performance to be analysed.	**Must**
SMR.040	Service Management and Service Integration	**Problem Management**	The Supplier must provide Problem Management Resource that is a subject matter expert with experience of working in a complex multi-supplier IT environment.	**Must**
SMR.041	Service Management and Service Integration	**Problem Management**	The Supplier must provide a staffing model that will expand when volumes increase over thresholds based on forecasted volumes at the solutioning time. The Supplier is responsible for forecasting and staffing accordingly to ensure levels of service are maintained.	**Must**
SMR.042	Service Management and Service Integration	**Problem Management**	The Buyer reserves the right to determine a "problem" (as defined in "SMSI-071-001-011 Defra Problem Management Policy") priority for any problem different to that assigned by the Supplier in the first instance, and the Supplier shall accept the Buyer mandated problem case priority.	**Must**
SMR.043	Service Management and Service Integration	**Problem Management**	The Supplier must diagnose using relevant tools to find pertinent information that helps troubleshoot the possible root cause(s) of the multiple Incidents and record all activity relating to the problem investigation, diagnosis and resolution in the Supplier's service management system (ITSM tool). The choice of diagnostic tools, method of investigation and recommendation for resolution, are the Supplier's responsibility.	**Must**
SMR.044	Service Management and Service Integration	**Problem Management**	The Supplier must execute Problem Management remediations within the agreed Service Levels as set out in the Call Off Schedule 3 (Service Levels, Service Credits and Performance Monitoring).	**Must**
SMR.045	Service Management and Service Integration	**Problem Management**	The Supplier must perform Root Cause Analysis ("RCA") and conduct a problem investigation to identify a permanent fix, as outlined within the Problem Management Policy & Process. Where a permanent fix is not possible, these deviations will be assessed in line with Buyer's risk appetite.	**Must**
SMR.046	Service Management and Service Integration	**Problem Management**	The Supplier must issue Root Cause Analysis ("RCA") reports to the Buyer for all Priority Level 1, Priority Level 2, Priority Level 3 and Priority Level 4 problems	**Must**
SMR.047	Service Management and Service Integration	**Problem Management**	Where there is no known route cause for Priority 1 and Priority 2 Incidents, the Supplier must generate a problem record within the Buyer's Service Levels in accordance with the Buyer's Problem Management Policy - "SMSI-071-001-011 Defra Problem Management Policy" and Problem Management Process - "SMSI-071-002-011 Defra Problem Management Process".	**Must**
SMR.048	Service Management and Service Integration	**Change Management**	The Supplier must operate Change Management in accordance with the Buyer's Change and Evaluation Management Policy (SMSI-071-001-003) and Change and Evaluation Management Process (SMSI-071-002-003).	**Must**
SMR.049	Service Management and Service Integration	**Change Management**	An Operational Change is defined as any change which falls under the Buyer's Change and Evaluation Management Policy (SMSI-071-001-003) and Change and Evaluation Management Process (SMSI-071-002-003).	**Must**
SMR.050	Service Management and Service Integration	**Change Management**	Operational Changes which do not affect the pricing structure under the Contract and / or other terms of the Contract will not constitute changes for the purposes of the variation procedure set out in the Contract (and accordingly, will not be subject to additional Charges or expenses).	**Must**
SMR.051	Service Management and Service Integration	**Change Management**	The Supplier must adhere to the Buyer's Change and Evaluation Management process (SMSI-071-002-003) whereby all planned changes to the Buyer's environment(s) are communicated to the Buyer following the change types and lead times within the Buyer's Change and Evaluation Management Process (SMSI-071-002-003).	**Must**
SMR.052	Service Management and Service Integration	**Change Management**	The Supplier must adhere to the Buyer's Change and Evaluation Management process (SMSI-071-002-003) whereby all Emergency changes to the Buyer's environment(s) are communicated to the Buyer to ensure that critical changes can be applied within the agreed emergency implementation window as set-out within the Contract resolution SLA targets.	**Must**
SMR.053	Service Management and Service Integration	**Change Management**	The supplier must participate in the Buyer's Change Advisory Board and Emergency Change Advisory Board which will include as required: (a) attending CAB and ECAB meetings; (b) reviewing RFCs and eRFCs; (c) providing impact and risk assessments on RFCs and eRFCs; and (d) submitting proposed RFCs and eRFCs for review	**Must**
SMR.054	Service Management and Service Integration	**Change Management**	All Operational Changes must be approved by the set of stakeholders agreed by the Buyer prior to implementation of the changes proceeding.	**Must**
SMR.055	Service Management and Service Integration	**Change Management**	The supplier must gain authorisation for Emergency Changes from the Buyer's Emergency Change Advisory Board to implement Emergency Changes in accordance with the Buyer's Change and Evaluation Management Policy (SMSI-071-001-003) and Change and Evaluation Management Process (SMSI-071-002-003)	**Must**
SMR.056	Service Management and Service Integration	**Change Management**	The supplier must provide a single point of contact for the review and approval of all Operational Changes and for the coordination of Operational Changes with other suppliers.	**Must**
SMR.057	Service Management and Service Integration	**Change Management**	The Supplier must communicate to the Buyer any unauthorised Operational Changes as soon as they are identified, with details on the impact of the change.	**Must**
SMR.058	Service Management and Service Integration	**Change Management**	The Supplier must communicate to the Buyer any planned/unplanned outages associated with Operational Changes .	**Must**
SMR.059	Service Management and Service Integration	**Change Management**	The Supplier must plan maintenance activities in order to minimise disruption to production services from Operational Changes.	**Must**
SMR.060	Service Management and Service Integration	**Change Management**	The supplier must follow the Buyer's Change and Evaluation Management process (SMSI-071-002-003) for the resolution of incidents or major incidents where a change is required to an operational environment.	**Must**
SMR.061	Service Management and Service Integration	**Change Management**	The Supplier must continue to proactively monitor the Service during any outage (planned or unplanned) and regularly report back and provide updates to the Buyer's Change Manager, Incident Manager and Service Owner.	**Must**
SMR.062	Service Management and Service Integration	**Change Management**	The Supplier must provide Early engagement for new services to understand how change management will be executed and ensure all key info is collated	**Must**
SMR.063	Service Management and Service Integration	**Change Management**	The Supplier must provide regular and ad hoc targeted reporting to allow the effectiveness of change management performance to be analysed.	**Must**
SMR.064	Service Management and Service Integration	**Change Management**	The Supplier must provide a change management Resource that is a subject matter expert with experience of working in a complex multi-supplier IT environment.	**Must**

SMR.065	Service Management and Service Integration	**Change Management**	The supplier must provide a staffing model that will expand when volumes increase over thresholds based on forecasted volumes at the solutioning time.	**Must**
SMR.066	Service Management and Service Integration	**Release and Deployment Management**	The supplier must operate Release and Deployment procedures in adherence with to the Buyer's Release and Deployment Management Policy (SMSI-071-001-012) and Release and Deployment Management Process (SMSI-071-002-012).	**Must**
SMR.067	Service Management and Service Integration	**Release and Deployment Management**	For Client Deployments, the Supplier must ensure that any planned upgrades and/or releases are communicated to the Buyer at least thirty (30) days in advance of them being deployed.	**Must**
SMR.068	Service Management and Service Integration	**Release and Deployment Management**	The Supplier must keep the Buyer updated with a weekly forward view of Service Roadmaps, the Forward Schedule of Release, and Architectural Roadmaps, and any planned Service enhancements or Service updates, ensuring that the Buyer is an informed customer. This includes providing weekly updates on Release activities.	**Must**
SMR.069	Service Management and Service Integration	**Release and Deployment Management**	The supplier must provide Early Life Support plans to the Buyer and adhere to the Release and Deployment Management Process (SMSI-071-002-012) for the deployment of new Services or changes to Services prior to Service Commencement Date.	**Must**
SMR.070	Service Management and Service Integration	**Release and Deployment Management**	The Supplier should provide a named Change and Release Manager as a point of contact for the Buyer.	**Should**
SMR.071	Service Management and Service Integration	**Release and Deployment Management**	The supplier must provide a detailed status and availability report on all lower-level/test environments. Status reports must include the environment versions and any planned upgrades due to be implemented to the environment, inline with the Release and Deployment Management Process (SMSI-071-002-012) . Lower-level/test environments include (but are not limited to), SND, TEST, PRE-PROD.	**Must**
SMR.072	Service Management and Service Integration	**Release and Deployment Management**	The Supplier must communicate and provide environment plans to the Buyer to avoid any potential conflict with Release's and downtime, including communicating key project commitments, plans, Changes and Project Requirements.	**Must**
SMR.073	Service Management and Service Integration	**Request Fulfilment**	The Supplier must use Buyer's ITSM toolset, in the management and execution of the Request Fulfilment process. This includes, but is not restricted to: •An End User submitting a request through the IT Service Catalogue web interface / portal •A Request for Change (RFC) requires a Service Request to be fulfilled as part of the change implementation •An Incident results in the need to request a new service or product via the Request Fulfilment process	**Must**
SMR.074	Service Management and Service Integration	**Request Fulfilment**	The supplier must maintain the Approved Request Fulfilment procedures in accordance with the Buyer's Request Fulfilment Policy (SMSI-071-001-014) and Request Fulfilment Process (SMSI071-002-014), with the handling of Service Requests from their submission to validation, approval, fulfilment, closure and cancellation, thereby providing a channel for End Users to request and receive standard products and services and sourcing and delivering the components of requested standard services.	**Must**
SMR.075	Service Management and Service Integration	**Request Fulfilment**	The Supplier must support and adhere to the Buyer's Request Fulfilment process for prioritisation and escalation of VIP user requests. The Supplier must treat these requests as priority requests when instructed by the Buyer and provide escalated support when requested by the Buyer. VIPs consist of, but not limited to, Senior Officials, Ministerial Teams, Director Generals, Chief Operating Officers, Senior Civil Servant and Assitive Technology Users.	**Must**
SMR.076	Service Management and Service Integration	**Request Fulfilment**	The Supplier must provide proactive updates on all Service Requests to the end user with information on the status and progress with the request, including any changes in delivery dates, as well as responding to enquiries that are submitted by the end user through the Buyer's Service Desk provider via the Service Catalogue ITSM toolset. The Supplier must provide the end user with a clear descriptive progress status update, in relation to their fulfilment requests.	**Must**
SMR.077	Service Management and Service Integration	**Request Fulfilment**	The Supplier must escalate and manage escalated tickets to the Buyer on any requests identified as not being resolved within their agreed service levels.	**Must**
SMR.078	Service Management and Service Integration	**Request Fulfilment**	The Supplier must submit requests on behalf of customers when contacted, and must log requests through the Buyer's Service Desk provider via the Service Catalogue ITSM toolset, currently this is ServiceNow (MyIT).	**Must**
SMR.079	Service Management and Service Integration	**Request Fulfilment**	The Supplier must ensure the Request item is operational for the user, and must confirm directly with the End User, ensuring acceptance of delivery before the ticket is closed.	**Must**
SMR.079	Service Management and Service Integration	**Service Catalogue Management**	The supplier must operate Service Catalogue Management in accordance with the Buyer's Service Catalogue Management Policy (SMSI-071-001-018) and Service Catalogue Management Process (SMSI-071-002-018).	**Must**
SMR.080	Service Management and Service Integration	**Service Catalogue Management**	The supplier must publish and maintain the Services in the Service Catalogue in accordance with the Buyer's Service Catalogue Management Policy (SMSI-071-001-018) and Service Catalogue Management Process (SMSI-071-002-018).	**Must**
SMR.081	Service Management and Service Integration	**Service Catalogue Management**	The supplier must share and demonstrate Catalogue Items that can be procured or purchased to include as part of the Buyer's catalogue offering, in alignment with the Buyer's Request Fulfilment Process (SMSI-071-002-014). Management reports shall be provided to both demonstrate the effective use of the catalogue and enable analysis of demand to enable proactive calatlogue management.	**Must**
SMR.082	Service Management and Service Integration	**Access Management**	The supplier must operate Access Management in accordance with the Buyer's Access Management Policy (SMSI-071-001-013) and Access Management Process (SMSI-071-002-013).	**Must**
SMR.083	Service Management and Service Integration	**Access Management**	The supplier must allow the Buyer access upon request to audit trails and logs of Access Requests to Services.	**Must**
SMR.084	Service Management and Service Integration	**Knowledge Management**	The supplier must operate Knowledge Management procedures in accordance with the Buyer's Knowledge Management Policy (SMSI-071-001-009) and Knowledge Management Process (SMSI-071-002-009) for the Services	**Must**
SMR.085	Service Management and Service Integration	**Knowledge Management**	The supplier must maintain Knowledge Articles in adherence to the Buyer's Knowledge Management Policy (SMSI-071-001-009) and Knowledge Management Process (SMSI-071-002-009) for the Services.	**Must**



SMR.086	Service Management and Service Integration	**ITSM Tooling**	The Supplier must use the Buyer's IT Service Management toolset, (currently this is ServiceNow), and those processes currently supported through the toolset in the delivery of the Supplier's service to the Buyer. The processes currently supported through the Buyer's toolset include (but not limited to): (a) Access Management; (b) Change and Evaluation Management; (c) Incident Management and Major Incident Management; (d) Knowledge Management; (e) Problem Management; (f) Release and Deployment Management; (g) Request Fulfilment; (h) Service Level Management. (i) Service Asset (Hardware and Software) and Configuration Management; (j) Service Catalogue Management; (k) Availability Management; (l) Capacity Management; (m) Demand Management;	**Must**
SMR.087	Service Management and Service Integration	**ITSM Tooling**	Where deemed appropriate by the Buyer, the Supplier must use the following ServiceNow modules in accordance with the Buyer's Service Management policies and processes and ServiceNow best practice; these modules are (but not limited to): (a) IT Service Management (ITSM); (b) IT Operations Management (ITOM); (c) Hardware Asset Management (HAM); (d) Software Asset Management (SAM); (e) Customer Service Management (CSM); (f) Discovery (g) Knowledge Management Repository (h) Certificate Lifecycle Management (i) LANSweeper Integration (j) ITOM Discovery (k) ITOM Service Mapping (l) ITOM Certificate Management (m) ITOM Automation and Orchestration (n) ITOM Health (Event Management) (o) Hardware Asset Management (p) Software Asset Management (q) Intune (r) Now Agent (s) Survey Management (t) Automated Test Framework (u) Continual Improvement Management	**Must**
SMR.088	Service Management and Service Integration	**ITSM Tooling**	The Supplier must use the Buyer's instance of the IT Service Management toolset, (currently this is ServiceNow) as the primary source of truth. Instance to instance integration is prohibited. The Buyer will consider integrations with 3rd party tools where this does not require the creation of any customisations.	**Must**
SMR.089	Service Management and Service Integration	**ITSM Tooling**	The Supplier must provide and maintain all system management, monitoring and administration tools required for the provision of the Services and Modules.	**Must**
SMR.090	Service Management and Service Integration	**ITSM Tooling**	The supplier must use system management, monitoring and administration tools in the delivery of their Services with the ITSM Toolset and Enterprise Service Management Toolset in accordance with the Buyer's policies, processes and procedures.	**Must**
SMR.091	Service Management and Service Integration	**ITSM Tooling**	The supplier must make available tools, systems and associated capabilities including the provision of training in connection with the use of such tools, to the Service Desk Supplier to enable First Contact Resolution for Services, prior to the Operational Service Commencement Date applicable to those Services.	**Must**
SMR.092	Service Management and Service Integration	**ITSM Tooling**	The Supplier must ensure appropriate delegation of rights to access the Suppliers tools, systems and associated capabilities to enable the Service Desk Supplier to perform First Contact Resolution for agreed Incidents and Service Requests, including End User access requests.	**Must**
SMR.093	Service Management and Service Integration	**ITSM Tooling**	The Supplier must provide information that aligns with the Buyer's Common Service Data Model (CSDM) that underpins the CMDB as the central source for all data relating to the Services provisioned by the Buyer.	**Must**
SMR.094	Service Management and Service Integration	**ITSM Tooling**	The Supplier must ensure that any data held in the Configuration Management Database (CMDB) is accurate and up-to-date.	**Must**
SMR.095	Service Management and Service Integration	**ITSM Tooling**	The Supplier must provide periodic Management Information on the data held within the Configuration Management Database (CMDB) relating to their Service.	**Must**
SMR.096	Service Management and Service Integration	**Event Management**	Using Event Monitoring tools, the supplier must effectively operate Event Management, this includes but is not limited to; •Conducting proactive monitoring, •Pre-emptive fault identification, •Review alerts and events to manage the health, availability, and performance of the Service that the Supplier supports. The Supplier must immediately remediate all detectable and discernible Event occurrence/monitoring/alert notifications, evaluate the impact of deviation caused to the Service and rectify the deviation to restore normal service operation, within the Service Level Agreement (SLA). The Supplier must provide assurances to the Buyer through each stage of the Event lifecycle as outlined in the Buyer's Event Management Policy (SMSI-071-001-005) and Event Management Process (SMSI-071-002-005). The Buyer will consider integrations with 3rd party monitoring tools where this does not require the creation of any customisations to the ITSM Tool and adheres to the Buyer's Tooling Policies and Standards.	**Must**
SMR.097	Service Management and Service Integration	**IT Business & Service Continuity Management**	The Supplier must operate IT Service Continuity (ITSC) Management in accordance with the Buyer's IT Service Continuity Management Policy - 'SMSI-071-001-008 Defra Service Continuity Management Policy' and IT Service Continuity Management Process - 'SMSI-071-002-008 Defra Service Continuity Management Process', and in accordance with Call Off Schedule 16.	**Must**
SMR.098	Service Management and Service Integration	**IT Business & Service Continuity Management**	The Supplier must invoke the relevant ITSC plan when the occurrence of an ITSC event has been approved by the Buyer.	**Must**



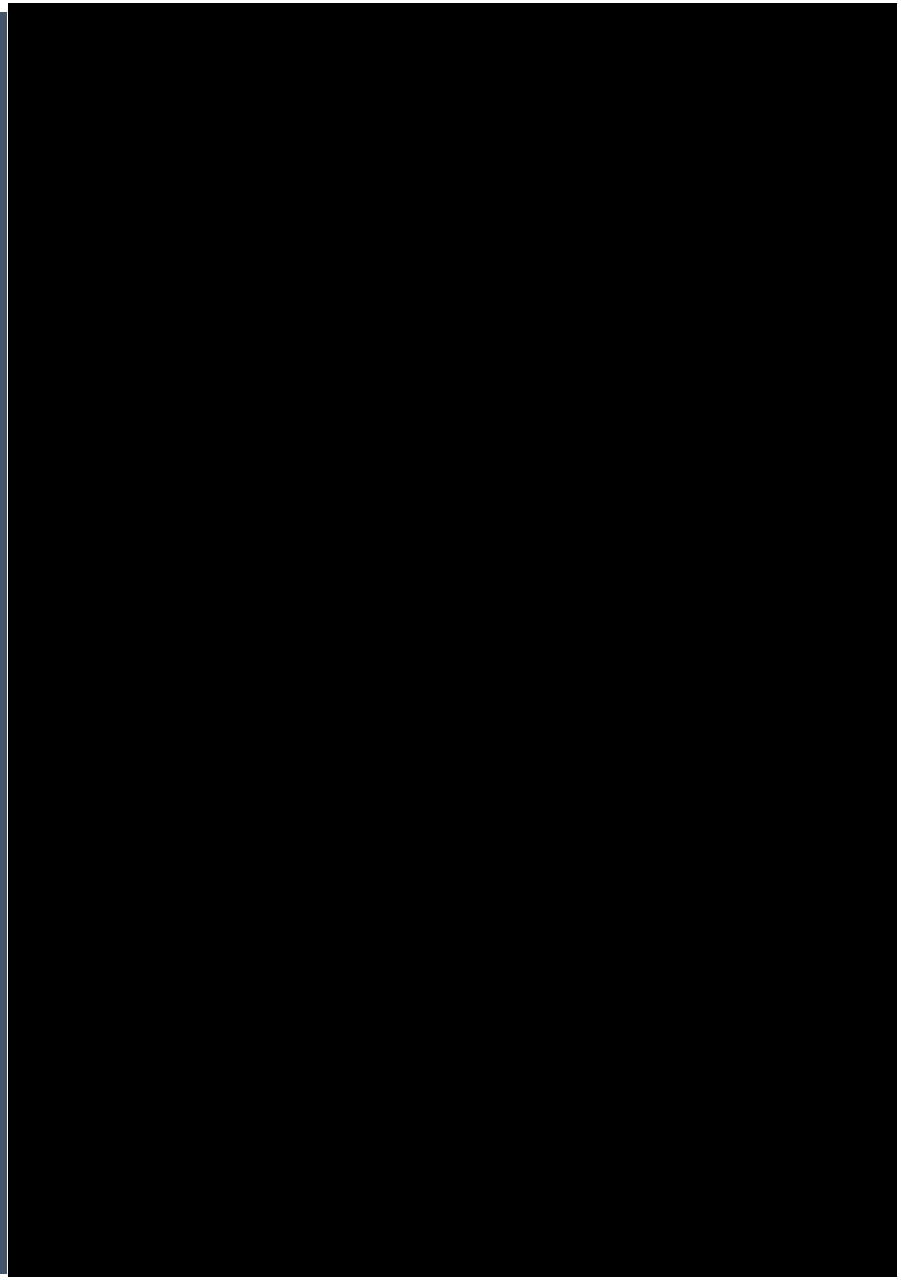
SMR.099	Service Management and Service Integration	**IT Business & Service Continuity Management**	The Supplier must close the relevant ITSC plan on receipt of approval from the Buyer, that the ITSC event has been successfully mitigated.	**Must**
SMR.100	Service Management and Service Integration	**IT Business & Service Continuity Management**	The Supplier must, following the closure of an ITSC Plan, provide to the Buyer within twenty (20) Working Days of the ITSC Plan closure an ITSC Event report detailing the activities undertaken to restore the Services and potential changes to the Services that could help reduce the likelihood of the same ITSC Event or a similar ITSC Event happening in the future.	**Must**
SMR.101	Service Management and Service Integration	**IT Business & Service Continuity Management**	The Supplier must ensure that the levels of resilience and redundancy within the Services are effectively monitored and maintained. The Supplier must notify the Buyer within 2 hours of all events that result in loss of resilience to the Services provided by the Supplier to the Buyer.	**Must**
SMR.102	Service Management and Service Integration	**IT Business & Service Continuity Management**	The Supplier must identify and mitigate risks or threats to business operations from specific events, including as a minimum, major international events, pandemics, malicious attacks, natural hazards,	**Must**
SMR.103	Service Management and Service Integration	**IT Business & Service Continuity Management**	The Supplier must have in place, and share with the Buyer, a business continuity strategy for the Services, including as a minimum, people, premises, technology, information, Suppliers and stakeholders.	**Must**
SMR.104	Service Management and Service Integration	**IT Business & Service Continuity Management**	The Supplier must have regularly updated business continuity arrangements that include business continuity incident management process, notification processes, recovery strategy/procedures and the estimated recovery time for products/services. These requirements are to be carried out in accordance with the ITSC and BCDR plans.	**Must**
SMR.105	Service Management and Service Integration	**IT Business & Service Continuity Management**	The BCDR Plan must identify and document contingencies to mitigate the impact on the Services of an incident (including loss of your people, products/services and supplies).	**Must**
SMR.106	Service Management and Service Integration	**IT Business & Service Continuity Management**	The Supplier must ensure that they have updated any plans, policies and processes to reflect any lessons learnt from testing and/or invocation including any lessons learnt from the COVID-19 pandemic.	**Must**
SMR.107	Service Management and Service Integration	**IT Business & Service Continuity Management**	The Services and Goods must be resilient to climate change risks, such as storms, flooding, disrupted travelling conditions and power supplies, and ambient temperature increases, e.g. designing goods that can operate in extreme temperatures. The Supplier must consider how extreme weather events and a changing climate could affect its ability to source the products or deliver the services required under this contract as part of its business continuity planning.	**Must**
SMR.108	Service Management and Service Integration	**IT Business & Service Continuity Management**	During times of national emergency e.g. national flood or disease outbreak, the Supplier must be able to work closely with the Buyer to ensure operational and extended or expanded service and continuity of service is achievable, as deemed appropriate by the Buyer.	**Must**
SMR.109	Service Management and Service Integration	**Capacity Management**	The supplier must operate Capacity Management for the Services in accordance with the Buyer's Capacity Management Policy (SMSI-071-001-002) and Capacity Management Process (SMSI-071-002-002).	**Must**
SMR.110	Service Management and Service Integration	**Capacity Management**	The supplier must produce and make available, via the Service Knowledge Management System (ServiceNow), to the Buyer monthly Capacity Reports on a per site basis which include: (a) current resource utilisation; (b) resource utilisation trends and forecasts; and (c) issues and exceptions (d) in accordance with the Buyer's Capacity Management Policy (SMSI-071-001-002) and Capacity Management Process (SMSI-071-002-002)	**Must**
SMR.111	Service Management and Service Integration	**Capacity Management**	The supplier must develop, monitor, track and complete Approved remediation action plans to address any Capacity deficiency or surplus in accordance with the Buyer's Capacity Management Policy (SMSI-071-001-002) and Capacity Management Process (SMSI-071-002-002), or as otherwise agreed with the Buyer.	**Must**
SMR.112	Service Management and Service Integration	**Capacity Management**	The Supplier must undertake proactive monitoring of capacity and trends including use of predictive modelling and recommend any required optimisation of the capacity to accommodate the Buyer's business requirements, future developments and growth forecasts.	**Must**
SMR.113	Service Management and Service Integration	**Capacity Management**	The Supplier must proactively monitor the Buyer's Service availability and capacity utilisation on a 24 hours per day, 365 days a year (366 days in a leap year) basis and the breaching thereof.	**Must**
SMR.114	Service Management and Service Integration	**Capacity Management**	The Supplier must ensure that when the Service is operating in a degraded state e.g. only one data centre is operating, then the Service must still have sufficient capacity to accommodate the Buyer's business requirements.	**Must**
SMR.115	Service Management and Service Integration	**Capacity Management**	The Supplier must report actual capacity status to the service owner on a monthly basis via a rolling 12 month report including limits and capacity thresholds, consumption, utilisation trends, peak usage and risks	**Must**
SMR.116	Service Management and Service Integration	**Capacity Management**	The Supplier must include on the agenda for the monthly Performance Review Meetings, a review of the performance and capacity of the Service including any risks or breaches and the Rectification Plan for any breaches.	**Must**
SMR.117	Service Management and Service Integration	**Capacity Management**	The Supplier must develop roadmaps and plans for capacity improvement where the need for capacity upgrade is identified.	**Must**
SMR.118	Service Management and Service Integration	**Availability Management**	The supplier must operate Availability Management in accordance with the Buyer's Availability Management Policy (SMSI-071-001-001) and Availability Management Process (SMSI 071-002-001).	**Must**

SMR.119	Service Management and Service Integration	**Availability Management**	The supplier must utilise an Availability Management Information System (AMIS) able to document and maintain Availability Management data for the Services.	**Must**
SMR.120	Service Management and Service Integration	**Availability Management**	The Supplier must maintain 24/7, four nines (99.99%) availability for all **critical** Service, as defined by Schedule 3 (Service Levels, Service Credits and Performance Monitoring) and the scope of the services under this contract.	**Must**
SMR.121	Service Management and Service Integration	**Availability Management**	The Supplier must ensure that the solution is designed to meet the Buyer's Availability/uptime service levels as set out in the Contract Schedule.	**Must**
SMR.122	Service Management and Service Integration	**Availability Management**	The Supplier must perform availability management to carry out performance monitoring and optimisations of the Service so as to deliver a sustained level of availability that as a minimum meets the availability service level set out in the Contract Schedule.	**Must**
SMR.123	Service Management and Service Integration	**Service Asset and Configuration Management**	The Supplier must ensure the information held for Configuration Items within the Supplier scope, Software and Hardware Assets used to deliver the Services is accurate, providing updates and new information as necessary in accordance with the Buyer's: (a) Software Asset Management Policy (SMSI-071-001-017) and Software Asset Management Process (SMSI-071-002-017) b) Hardware Asset Management Policy (SMSI-071-001-016) and Hardware Asset Management Process (SMSI-071-002-016); and (c) Configuration Management Policy (SMSI-071-001-015) and Configuration Management Process (SMSI-071-002-015).	**Must**
SMR.124	Service Management and Service Integration	**Service Asset and Configuration Management**	The Supplier must maintain accurate records of Configuration Items within the Supplier scope, Software and Hardware Assets used to deliver the Services in accordance with the Buyer's: (a) Software Asset Management Policy (SMSI-071-001-017) and Software Asset Management Process (SMSI-071-002-017); (b) Hardware Asset Management Policy (SMSI-071-001-016) and Hardware Asset Management Process (SMSI-071-002-016); and (c) Configuration Management Policy (SMSI-071-001-015) and Configuration Management Process (SMSI-071-002-015).	**Must**
SMR.125	Service Management and Service Integration	**Service Asset and Configuration Management**	The Supplier must raise a Request for Change via the Buyer's Change and Evaluation Management Policy (SMSI-071-002-003) for all changes to a Configuration Item or Asset.	**Must**
SMR.126	Service Management and Service Integration	**Service Asset and Configuration Management**	The Supplier must conform to the Buyer's Common Services Data Model and ensure that Configuration Items are uniquely identified and defined by attributes that describe their functional and physical characteristics as defined by the Buyer's Common Services Data Model. The Supplier shall support deployment and operation of Defra's discovery tooling and the provision of all relevant credentials and permissions required for that tooling to both discover and create an inventory all software and hardware Assets and Configuration Items within the Defra estate	**Must**
SMR.127	Service Management and Service Integration	**Service Asset and Configuration Management**	The Supplier must ensure that the Configuration Management Database (CMDB) is updated within two (2) Working Days following the: - Implementation of a Change - Resolution of Incidents; and/or - Completion of a Service Request	**Must**
SMR.128	Service Management and Service Integration	**Service Measurement and Reporting**	The supplier must operate Service Measurement and Reporting procedures in accordance with the Buyer's Service Measurement and Reporting Policy (SMSI-071-001-020) and Service Measurement and Reporting Process (SMSI-071-002-020).	**Must**
SMR.129	Service Management and Service Integration	**Service Measurement and Reporting**	The Supplier must provide periodic Management Information in support of Service Levels, Experience Levels and Key Performance Indicators as set out in the Call Off Schedule 3 (Service Levels, Service Credits and Performance Monitoring).	**Must**
SMR.130	Service Management and Service Integration	**Service Measurement and Reporting**	The Supplier must engage with the Buyer's performance reporting function and attend governance boards, such as Service Management Board's as identified in the Contract Schedules.	**Must**
SMR.131	Service Management and Service Integration	**Service Measurement and Reporting**	The Supplier must provide Service Management reporting on Service Performance against SLAs, XLAs and KPIs, exceptions, risks and issues, CSI, Change and Problem, Security and compliance, supported by raw data where required by the Buyer.	**Must**
SMR.132	Service Management and Service Integration	**Service Measurement and Reporting**	The Supplier must use Buyer's ITSM toolset, currently this is ServiceNow (MyIT) for operational processes and service performance reporting against SLAs, in the management and execution of the following Service Management processes: (a) Access Management; (b) Change and Evaluation Management; (c) Incident Management; (d) Knowledge Management; (e) Release & Deployment Management; (f) Request Fulfilment; and (g) Service Level Management (h) Security Management (i) Service Asset and Configuration Management.	**Must**
SMR.133	Service Management and Service Integration	**Service Level Management**	The supplier must operate Service Level Management procedures, in accordance to the Buyer's Service Level Management Policy (SMSI-071-001-019) and Service Level Management Process (SMSI-071-002-019).	**Must**
SMR.134	Service Management and Service Integration	**Service Level Management**	The Supplier must provide SLA reporting for the reporting period as required by the Buyer, showing details of attainment/breach of contractual Service Levels (as detailed in Call Off Schedule 3 (Service Levels, Service Credits and Performance Monitoring)).	**Must**
SMR.135	Service Management and Service Integration	**Service Level Management**	The Supplier must attend and participate with Service Level Reviews held by the Buyer. The Buyer reserves the right to modify SLAs to the Service and Supplier Management Process, including underpinning agreements, underpinning contracts and OLAs.	**Must**

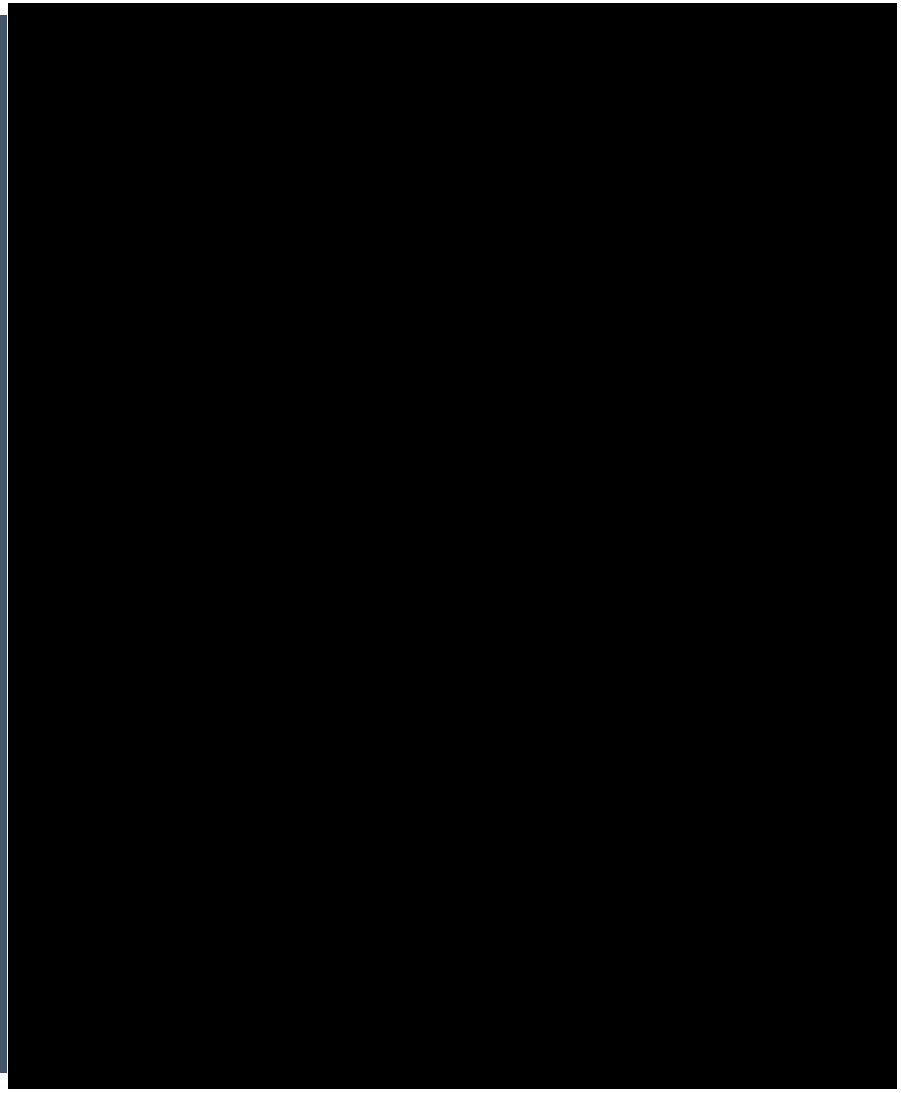
[redacted]

SMR.136	Service Management and Service Integration	**Service Experience**	For the Service Desk End User provision, the Supplier must implement Digital Experience (DEX) Tooling incorporated into the ITSM toolset, ServiceNow (MyIT) in order to provide: 1. Digital experience reporting to support XLA reporting; 2. Efficient ticket handling; 3. Pre-emptive fault identification; 4. Directed user initiated resolution action and auto ticketing.	**Must**
SMR.137	Service Management and Service Integration	**Service Experience**	For all other Services outside of the Service Desk End User Provision, the Supplier should implement customer/user experience tooling or a combination of tools incorporated into the ITSM toolset, ServiceNow (MyIT) in order to provide: 1. Digital experience reporting to support XLA reporting; 2. Efficient ticket handling; 3. Pre-emptive fault identification; 4. Directed user initiated resolution action and auto ticketing.	**Must**
SMR.138	Service Management and Service Integration	**Service Experience**	The Supplier must coordinate and collaborate with the Buyer and other contractors and its customers to build, measure and report on Experience Level Agreements and Experience Level indicators based on performance of users service actions; performance of user interfaces and user satisfaction with the overall service and specific components of the service or actions. These XLAs must be based on a combination of sentiment reporting such as customer surveys, digital experience using Digital Experience Tools and performance reporting.	**Must**
SMR.139	Service Management and Service Integration	**Service Experience**	End User Experience must be a primary consideration for the Supplier and any Business engagement approach must include; but not limited to: •Business Relationship Managers and Service Experience Managers- ensuring that the interests of the Core Department and each Arms-Length Body are fully represented; •Business and IT Service Owners Intelligent Customer Functions representing Arm's Length Bodies IT users Business Analysts and User Researchers; •Suppliers as appropriate	**Must**
SMR.140	Service Management and Service Integration	**Continual Service Improvement**	The Supplier must operate Continual Service Improvement in accordance with the Buyer's Service Improvement Policy (SMSI-071-001-004) and Service Improvement Process (SMSI-071-002-004).	**Must**
SMR.141	Service Management and Service Integration	**Continual Service Improvement**	The Supplier must raise Service Improvement opportunities for the Services in accordance with the Buyer's Service Improvement Policy (SMSI-071-001-004) and Service Improvement Process (SMSI-071-002-004)	**Must**
SMR.142	Service Management and Service Integration	**Continual Service Improvement**	The Supplier must demonstrate quality output and responsibility for the management of Continual Service Improvement initiatives for all service related activities whether these are generated from existing services that need improvement, new services that are introduced, services that are changed or based on service innovation that will improve the overall performance of existing ICT Service. The Buyer reserves the right to determine management of future ideas and innovation that would have the potential to create a significant shift in the cost and quality of delivering the IT Services to incentivise public spending.	**Must**
SMR.143	Service Management and Service Integration	**Continual Service Improvement**	The Supplier must showcase innovation ideas product roadmaps to enhance new and better ways of working with new innovative technologies that are trending by market experts, and contribute to cost-effective delivery models together with improving the quality of service, performance and experience.	**Must**
SMR.144	Service Management and Service Integration	**Risk Management**	The Supplier must manage risks to the delivery of the Services in accordance with the Buyer's Risk Governance procedures and the Operational Risk Management Policy (SMSI-071-001-010) and Risk Management Process (SMSI-071-002-010).	**Must**
SMR.145	Service Management and Service Integration	**Risk Management**	The Supplier must undertake risk management on a regular/ continual basis to identify any emergent risks to the provision of the Services and report these to the Buyer in accordance with Call Off Schedule 7 (Governance).	**Must**
SMR.146	Service Management and Service Integration	**Risk Management**	The Supplier must undertake regular proactive identification of risks to service and security, assess the potential impact of the risk, identify possible actions for the containment of the risk and work with Buyer to agree the appropriate course of action.	**Must**
SMR.147	Service Management and Service Integration	**Risk Management**	The Supplier must provide visibility, understanding and transparency of all risk ownership, mitigation and management related to the Services.	**Must**
SMR.148	Service Management and Service Integration	**Risk Management**	The Supplier must regularly document and update the Risk Register with risks and issues identified under the services/processes set out in the Call Off Contract Schedule 7 (Governance). The Supplier must keep the Risk Register up to date with the categorisation and priority as deemed appropriate by the Buyer, and submit it for review to the appropriate Boards.	**Must**
SMR.149	Service Management and Service Integration	**Risk Management**	The Supplier must conform to the Risk Governance routes as set out by the Buyer for any risk Escalations.	**Must**
SMR.150	Operational Services: Service Management and Service Integration	**Enterprise Architecture**	The supplier must following request by the Buyer, cooperate with and assist the Buyer in relation to the Services to create and / or update the Buyer's IT Roadmap for the Services.	**Must**
SMR.151	Operational Services: Service Management and Service Integration	**Enterprise Architecture**	The supplier must produce and make available to the Buyer for Approval, within a rolling six (6) months of the Call Off Commencement Date, an IT Roadmap for its Services in accordance with the Buyer's Enterprise Architecture Principles.	**Must**
SMR.152	Operational Services: Service Management and Service Integration	**Enterprise Architecture**	The supplier must update the IT Roadmap for its Services in accordance with the Buyer's Enterprise Architecture Principles and submit to the Buyer for Approval, on a biannual basis.	**Must**
SMR.153	Operational Services: Service Management and Service Integration	**Enterprise Architecture**	The supplier must ensure that the design of Services conform to the Buyer's Enterprise Architecture Principles.	**Must**
SMR.154	Operational Services: Service Management and Service Integration	**Enterprise Architecture**	The supplier must provide Architecture Artefacts in line with the Service Design Package, that describe the Services in accordance with the Buyer's Enterprise Architecture Principles and make them available to the Buyer, via the Service Knowledge Management System (ServiceNow) prior to each Operational Service Commencement Date.	**Must**

SMR.155	Operational Services: Service Management and Service Integration	**Enterprise Architecture**	The supplier must update and maintain the Architecture Artefacts in accordance with the Buyer's Enterprise Architecture Principles, and the Buyer's Change and Evaluation Management Policy (SMSI-071-001-003) and Change and Evaluation Management Process (SMSI-071-002-003), and as a minimum annually and more frequently if requested by the Buyer.	**Must**
SMR.156	Operational Services: Service Management and Service Integration	**Solution Architecture and Design**	The supplier must comply with the Service Delivery Lifecycle (SMSI-223-001).	**Must**
SMR.157	Operational Services: Service Management and Service Integration	**Solution Architecture and Design**	The supplier must ensure all Service Design Packages approved under the Service Delivery Lifecycle (SMSI-223-001) are submitted to the Buyer for Approval via the Change and Evaluation Management Policy (SMSI-071-002-003) and are subsequently made available from the Buyer's Service Knowledge Management System within five (5) Working Days of Approval.	**Must**
SMR.158	Operational Services: Service Management and Service Integration	**Solution Architecture and Design**	The supplier must ensure all changes to the approved Service Design Packages are produced in accordance with the Buyer's Service Design and Service Transition and Change and Evaluation Management Policy (SMSI-071-001-003) and the Service Design and Service Transition and Change and Evaluation Management Process (SMSI-071-002-003).	**Must**
SMR.159	Operational Services: Service Management and Service Integration	**Service Readiness**	The Supplier must contribute to a full and approved Service Design Package to the Buyer, to then be transposed into an approved Service Operations Guide by the Buyer and made it available via the ITSM Toolset within ServiceNow, prior to the Operational Services Commencement Date.	**Must**
SMR.160	Operational Services: Service Management and Service Integration	**Delivery Portfolio Management**	The supplier must contribute to or manage and deliver Projects in accordance with: (a) Schedule XX (Governance); (b) Buyer's Project Management Framework; and (c) Buyer's Service Delivery Lifecycle (SMSI-223-001)	**Must**
SMR.161	Operational Services: Service Management and Service Integration	**Delivery Portfolio Management**	The supplier must deliver Projects in accordance with: (a) Call Off Schedule 7 (Governance); (b) Call Off Schedule 19 (Projects); (c) Buyer's Project Management Framework; and (d) Buyer's Service Delivery Lifecycle (SMSI-223-001).	**Must**
SMR.162	Operational Services: Service Management and Service Integration	**Delivery Portfolio Management**	The Supplier must respond to a Project Initiation Request (PIR) by the provision of a Project Proposal as outlined within the Call Off Schedule 19 (Projects).	**Must**
SMR.163	Operational Services: Service Management and Service Integration	**Roadmaps Infrastructure Reporting**	The Supplier must within three (3) months of the Commencement Date, produce and make available to the Buyer for review and endorsement, a technology dataset for all technology elements that the Supplier: •has previously provided or managed (i.e., since the Commencement Date); •currently provides or manages; •will provide or manage, evidencing how end of life technology will be replaced with supported technology until contractual obligations end.	**Must**
SMR.164	Operational Services: Service Management and Service Integration	**Roadmaps Infrastructure Reporting**	The Supplier must at 3 months from formal endorsement of the previous dataset, repeating until the expiry of the Initial Term of the Contract and any Extension Period, produce and make available to the Buyer for review and endorsement, a technology dataset for all technology elements as outlined SMR.160 above	**Must**
SMR.165	Operational Services: Service Management and Service Integration	**Roadmaps Infrastructure Reporting**	The Supplier must following an ad hoc request by the Buyer, produce and make available to the Buyer for review and endorsement, a technology dataset for all technology elements as outlined in SMR.160 above	**Must**
SMR.166	Operational Services: Service Management and Service Integration	**Roadmaps Infrastructure Reporting**	The Supplier must use the latest versions of the Buyer's templates: ARC-490-003 Supplier Infrastructure Technology Dataset Template Product Description, ARC-490-004 Supplier Infrastructure Technology Dataset Template, ARC-490-005 (Appendix 1) Infrastructure Technology Dataset Document Review Process Flow, and the ARC-490-006 Infrastructure Technology Dataset DRF Template, as approved by the Buyer's Technical Governance Board, to produce their technology dataset	**Must**
SMR.167	Operational Services: Service Management and Service Integration	**Roadmaps Infrastructure Reporting**	The Supplier must co-operate with the Buyer and other Suppliers to visualise end to end technology roadmaps and allow the Buyer to share these roadmaps with other Suppliers.	**Must**
SMR.168	Operational Services: Service Management and Service Integration	**Service Validation and Testing**	The supplier must manage, plan, coordinate and execute all scheduled Testing activities to ascertain that the Supplier Call Off Solution operates as required and deliver the overall functionality and performance expected in accordance with: (a) Call Off Schedule 12 (Testing Procedures); (b) Buyer's Testing Strategy; (c) Buyer's Service Validation and Testing Policy (SMSI-071-001-021) and Service Validation and Testing Process (SMSI-071-002-021); and (d) the functional, non-functional and performance requirements as specified in the Approved Service Design Package	**Must**
SMR.169	Operational Services: Service Management and Service Integration	**Service Validation and Testing**	The supplier must be responsible and accountable for the execution of all Testing activities relating to its Services	**Must**
SMR.170	Operational Services: Service Management and Service Integration	**Service Validation and Testing**	The supplier must be responsible and accountable for managing Test data, in compliance with data protection legislation, for Testing that pertain to its Services by carrying out activities including; (a) specifying the Test data, including its source, scope, volume and processing; and (b) capturing and recording Test results and the categorisation of Test Issues as agreed with the Buyer pursuant to the Service Validation and Testing Process (SMSI-071-002-021)	**Must**
SMR.171	Operational Services: Service Management and Service Integration	**Service Validation and Testing**	The supplier must request from the Buyer the provision and decommission of pre-production test environments relating to the Services	**Must**
SMR.172	Operational Services: Service Management and Service Integration	**Service Validation and Testing**	The supplier must operate Service Validation and Testing procedures and related tools in accordance with the Buyer's Service Validation and Testing Policy (SMSI-071-001-021), Service Validation and Testing Process (SMSI-071-002-021) and the Buyer's Testing Strategy (SMSI-163-008) for its Services.	**Must**



SMR.173	Operational Services: Service Management and Service Integration	**Service Validation and Testing**	The supplier must maintain a Service Validation and Testing procedures in accordance with the Buyer's Service Validation and Testing Policy (SMSI-071-001-021) and Service Validation and Testing Process (SMSI-071-002-021) and the Buyer's Testing Strategy (SMSI-163-008).	**Must**
SMR.174	Operational Services: Service Management and Service Integration	**Service Validation and Testing**	The supplier must nominate an assigned tester as single point of contact for testing activities relating to the Services.	**Must**
SMR.175	Operational Services: Service Management and Service Integration	**Service Validation and Testing**	The supplier must provide and maintain test environments to support the test activities as defined within the Buyer's Testing Strategy (SMSI-163-008) and Approved Test Plan.	**Must**
SMR.176	Operational Services: Service Management and Service Integration	**Service Validation and Testing**	The supplier must ensure risks of service failure and disruption through transition have been fully investigated and understood, recorded and agreed with the Buyer, with workarounds agreed with the Buyer and documented in the Known Error Database in accordance with the Buyer's Operational Risk Management Policy (SMSI-071-001-010) and Risk Management Process (SMSI-071-002-010).	**Must**
SMR.177	Operational Services: Service Management and Service Integration	**Accessibility and Assistive Technology**	The Supplier must: Comply with Web Content Accessibility Guidelines (WCAG) 2.1 AA or the latest version at time of development (not equivalents) Undertake and provide a copy of a 3rd party audit (conducted by the Buyer's Accessibility Team contracted 3rd party auditor) at their expense to prove compliance with WCAG 2.1AA, (or latest version at the time of development) before any software/OS release or update. This must include manual testing by AT users. Commit to resolve any accessibility issues identified (including once deployed) within 2 months SLA with no charge to Defra (Or ALB) Commit to share fixes with other customers Accept and agree that the latest version of WCAG standards will apply to the entire service whenever work is undertaken Ensure compliance with the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 including, but not limited to, timely publishing and updating of accessibility statement at no extra cost Demonstrate operability with the Defra Assistive Technology software; - Dragon - JAWS - MS Dictate - MS Magnify - MS Narrate - Read and Write - ZoomText	**Must**
SMR.178	Operational Services: Service Management and Service Integration	**Accessibility and Assistive Technology**	The Supplier must provide a named Assistive Technology Lead who will be accountable for the Suppliers Assistive Technology service and a point of contact at Supplier for the Buyer to engage with.	**Must**
SMR.179	Operational Services: Service Management and Service Integration	**Accessibility and Assistive Technology**	The Supplier staffing model must include (as a minimum) individual AT skills, experience and certified qualifications as defined by the Equality Act 2010 and recognised by leading Assistive Technology industry standards. Trained and proven experience in the Buyer's Corporate AT software includes (but not limited to): Dragon, Inspiration, JAWS, Mind Manager, Read and Write, RSI Guard and ZoomText.	**Must**
SMR.180	Operational Services: Service Management and Service Integration	**Accessibility and Assistive Technology**	The Supplier must work collaboratively with the Buyer's third party suppliers for the management and handling of Assistive Technology user incidents or requests.	**Must**
SMR.181	Operational Services: Service Management and Service Integration	**Accessibility and Assistive Technology**	The Supplier must provide the Assistive Technology end user with a clear descriptive progress status update, in relation to their Assistive Technology incidents or requests. This includes following up with the assigned the Supplier/Resolver to obtain the latest information.	**Must**
SMR.182	Operational Services: Service Management and Service Integration	**Accessibility and Assistive Technology**	The Supplier must carry out horizon scanning and showcase ideas and options relating to Assistive Technology. The Supplier must produce Product Roadmaps to enhance Assistive Technology User Experience and improve the quality of service performance through new innovative Assistive Technologies that are trending by market leaders. The Buyer reserves the right to determine management of future Assistive Technology ideas and innovation that would have the potential to create a significant shift in the cost and quality of delivering the IT Services to incentivise public spending.	**Must**
SMR.183	Operational Services: Service Management and Service Integration	**Accessibility and Assistive Technology**	The Supplier must implement and progress Continual Service Improvement (CSI) to identify areas for improvement and efficiencies that ensures the Buyer's Assistive Technology offering remains current and appropriate for its needs.	**Must**

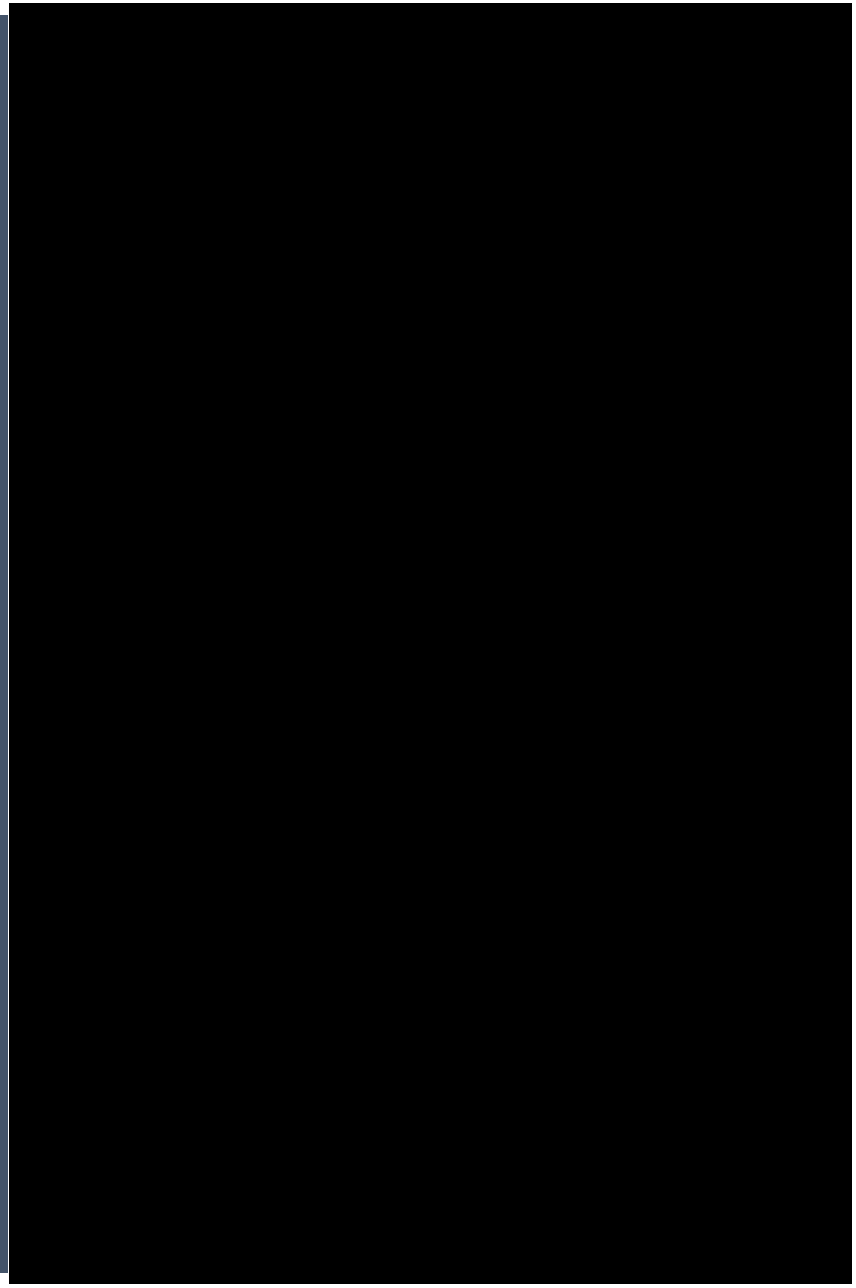


BUYER REQUIREMENTS					BIDDER COMPLIANCE RESPONSE	
ID	Operational Area	Service Function	Requirement	MoSCoW	Fully Compliant Partially Compliant Non-Compliant	COMPLIANCE STATEMENT [MAX 100 Words]
SEC.001	Information Security	**Security Management**	The Supplier must demonstrate any security certification (e.g. ISO27001, Cyber Essentials Plus) and provide independent certificates for validation.	**Must**		
SEC.002	Information Security	**Security Management**	The Supplier must ensure that all staff with access to Buyer information, data or systems are vetted to appropriate standards (minimum BPSS or national equivalent with elevated clearance levels for certain administrative role types to be agreed with the Buyer).	**Must**		
SEC.003	Information Security	**Security Management**	The Supplier must identify all third parties involved in the supplier's service, detail the services they provide and provide evidence that they will meet the same security standards of the Supplier. The Supplier shall ensure the flow-down to sub-contractors of contractual obligations.	**Must**		
SEC.004	Information Security	**Security Management**	The Supplier must provide details of the vulnerability management process relating to the systems processing or hosting Buyer information as part of the supplier's service.	**Must**		
SEC.005	Information Security	**Security Management**	The Supplier must agree to, and provide support for, an IT Health Check of the service carried out by an independent 3rd party under the NCSC CHECK Scheme prior to go live and at agreed intervals throughout the life of the Service. Vulnerabilities discovered as part of this activity will be remediated at the point in time in line with Buyer risk appetite. After agreeing the scope to the Buyer for review and approval, on completion the Supplier shall provide a Remedial Action Plan (RAP) detailing the timeline and actions to be taken to remediate any identified vulnerabilities.	**Must**		
SEC.006	Information Security	**Security Management**	The Supplier must make the Buyer aware of any significant changes to the service. Such changes might include re-hosting, architectural changes, major code changes or changes to support arrangements.	**Must**		
SEC.007	Information Security	**Security Management**	The Supplier must provide details on how the service is segregated from other customers so that the Buyer can determine whether the service is adequately protected.	**Must**		
SEC.008	Information Security	**Security Management**	The Supplier must provide details on how they will manage access control to ensure that access to Buyer data is limited to only that required for users to perform their roles.	**Must**		
SEC.009	Information Security	**Security Management**	All access to the service by Supplier staff must be logged and stored securely for an agreed period should analysis of this information be required.	**Must**		
SEC.010	Information Security	**Security Management**	The Supplier should provide evidence of management of the integrity of the service data , e.g. after a service outage.	**Should**		
SEC.011	Information Security	**Security Management**	The Supplier must provide evidence of monitoring for unusual activity and maintenance of records of events for future analysis and make available any logs and audit data relating to the service if required by the Buyer.	**Must**		
SEC.012	Information Security	**Security Management**	The Supplier must confirm that data will only be stored and processed for its intended purpose and that the storage and processing will comply with relevant legislation.	**Must**		
SEC.013	Information Security	**Security Management**	The Supplier must confirm that the service will be capable of supporting data up to a maximum protective marking of OFFICIAL, including the OFFICIAL-SENSITIVE handling caveat.	**Must**		
SEC.014	Information Security	**Security Management**	The Supplier must confirm that system data will not be shared with any other party without prior approval and that only the minimum data will be shared to meet the approved needs.	**Must**		
SEC.015	Information Security	**Security Management**	The Supplier should confirm that passwords and account management capabilities of the Service meet the standards set out in the Buyer's Password and Access Control Policy as a minimum.	**Should**		
SEC.016	Information Security	**Security Management**	The Supplier must detail any national or international supply chains upon which the service is dependent, to include software, hardware and/or services.	**Must**		
SEC.017	Information Security	**Security Management**	The Supplier shall indicate all reliance to offshored support and management of the service and what those offshored resources and locations will be. The Buyer may allow offshoring on a case-by-case basis. However, where the Supplier intends to use offshored support this shall be highlighted in the	**Must**		
SEC.018	Information Security	**Security Management**	The Supplier must provide evidence of adherence to established best practice such as adherence to security controls recommended by NCSC, OWASP, NIST, etc	**Must**		
SEC.019	Information Security	**Security Management**	The Supplier shall operate all of the in scope services in conformance with the Buyer's physical, information and Cyber security policies as well as any guidance set out by the NCSC. These policies will be amended and updated during the contract term and the Supplier shall continue to adhere to these security policies	**Must**		
SEC.020	Information Security	**Security Management**	The Supplier must provide support to the Buyer in its role as Data Controller of information provided to the supplier acting as a Processor. This includes information relating to appropriate organisational and technical controls put in place to secure the data, support for data subject's rights, compliance with data protection regulation, and only processing data as detailed in contracts and agreements with the Buyer	**Must**		

SEC.021	Information Security	**Security Management**	The Buyer shall have the right of audit, on provision of appropriate notice	**Must**
SEC.022	Information Security	**Security Management**	The Supplier shall develop and submit a Security Management Plan to the Buyer for review that covers the scope of the services provided to the Buyer and explains in detail how the Supplier will protect the Buyer's Information and information processing facilities	**Must**
SEC.023	Information Security	**Security Management**	The Supplier shall participate and comply with the Defra Group Security (DgS) security assurance process, including the use of tooling, providing security and privacy documentation and information, and mitigate risks to levels acceptable to the Buyer. This can be provided on request.	**Must**
SEC.024	Information Security	**Security Management**	The Supplier shall ensure the flow-down to sub-contractors of contractual obligations.	**Must**
SEC.025	Information Security	**Security Management**	When a Supplier processes health related information, and are in scope, they shall implement and provide assurance that they have completed the DSPT	**Must**
SEC.026	Information Security	**Security Management**	Suppliers shall have a robust incident response plan, which includes how they propose to work with the Buyer on incidents that impact Buyer data, systems, facilities, or personnel. The Supplier must provide details of the incident management process relating to security incidents involving Buyer information, data or systems.	**Must**
SEC.027	Information Security	**Security Management**	Suppliers shall have a robust business continuity plan, which includes how they propose to work with the Buyer on incidents that impact Buyer data, systems, facilities, or personnel	**Must**
SEC.028	Information Security	**Security Management**	The Supplier shall demonstrate their Secure Software Development Lifecycle (SSDLC) processes which include security and privacy by design and default. This shall include their vulnerability management, secure coding, release paths, testing, environment separation, and escalation through the environments	**Must**
SEC.029	Information Security	**Security Management**	The Supplier shall detail how they manage ongoing vulnerabilities in their systems, including any systems developed for the Buyer. The timeline for remediating vulnerabilities and risks posed shall also be provided to the Buyer	**Must**
SEC.030	Information Security	**Security Management**	The Supplier shall demonstrate their alignment to the BS EN ISO 19650-5:2020 standard when they are involved in building physical infrastructure	**Must**
SEC.031	Information Security	**Security Management**	The Supplier shall demonstrate their alignment to the ISO 23234:2021 standard when they are involved in building physical infrastructure	**Must**
SEC.032	Information Security	**Security Management**	If the Supplier processes payments on behalf of the Buyer, they shall demonstrate certification to Payment Card Industry - Data Security Standard (PCI-DSS) as well as providing assurance of the controls they have in place	**Must**
SEC.033	Information Security	**Security Management**	Where, the activity is likely to draw interest from specific threat actors, the Supplier shall have actions in their incident response plans to deal with and mitigate impacts from their activities.	**Must**
SEC.034	Information Security	**Security Management**	Where, the activity is likely to draw interest from specific threat actors, the Supplier shall have actions in their business continuity plans to deal with and mitigate impacts from their activities.	**Must**

BUYER REQUIREMENTS					BIDDER COMPLIANCE RESPONSE	
ID	Operational Area	Service Function	Requirement	MoSCoW	Fully Compliant Partially Compliant Non-Compliant	COMPLIANCE STATEMENT [MAX 100 Words]
DSK.001	Service Management and Service Integration	**Service Desk**	The Supplier must identify, record, categorise, prioritise, match and resolve incidents and requests (for First Contact Resolution (FCR), where possible). The Supplier must prioritise Tickets and assign correct severity classification in line with the Buyer guidelines as setout in the Incident Priority Matrix. The Supplier must assign, monitor, actively progress, escalate and close all incidents and requests raised through the Service Desk.	**Must**		[redacted]
DSK.002	Service Management and Service Integration	**Service Desk**	The Supplier must provide multiple communications channels for End Users to contact the Service Desk - These must include at Service Take On: Telephone access; Web portal / Self service capability; and Instant messaging chat Supplementary channels may be introduced during the Term (in agreement with the Buyer) including but not limited to: eMail, desktop nterface, Text contact, AI / Chat Bot.	**Must**		
DSK.003	Service Management and Service Integration	**Service Desk**	1. Within 5 days of a Known Error being made known, the Supplier must create, test and document work arounds that support teams can utilise where permanent fixes have not been implemented. 2. Any proposed workaround must be agreed with the Buyer in advance of use in the production environment.	**Must**		
DSK.004	Service Management and Service Integration	**Service Desk**	The Supplier must inform the Buyer as early as possible of any development activities on the tooling that supports the Service Desk. For example : Workflow enhancements Self help opportunities for Users Process refinements Any other initiatives that allow activities to 'shift left' in the support hierarchy	**Must**		
DSK.005	Service Management and Service Integration	**Service Desk**	1) The Supplier must ensure sufficient and appropriate staffing (trained, knowledgeable and security cleared) levels are maintained for the continuous delivery of Service Desk services to agreed service levels. This includes peak periods of activity and critical operational needs across the Buyer's business, which will require the Supplier to flex resource profiles in line with business demand. 2) The Supplier must provide full transparency as to the cost of the Service Desk, highlighting areas of efficiency opportunities that can be translated into cost savings or service improvement / value add initiatives.	**Must**		
DSK.006	Service Management and Service Integration	**Service Desk**	The Buyer will use the existing contact number for the Service Desk to minimise disruption to End Users. The Buyer will support the Supplier in porting this number from the incumbent Supplier to the incoming Supplier to use. The Supplier must ensure that the existing Buyer contact number is used for all telephony based contacts into the Service Desk.	**Must**		
DSK.007	Service Management and Service Integration	**Service Desk**	The Supplier must provide telephone access such that it can be utilised by staff with disabilities in accordance with applicable legislation and the Buyers IT Accessibility Standards.	**Must**		
DSK.008	Service Management and Service Integration	**Service Desk**	The Supplier must provide Service Desk support services across all channels 24x7. The Supplier must operate a Service Desk operated by UK based English speaking agents for telephony based interactions, resourced to meet agreed SLA's. Use of off-shore resources for non telephony based interactions must be in line with the Buyers off-shore usage policy	**Must**		

DSK.009	Service Management and Service Integration	**Service Desk**	The Supplier must provide telephony capability for the management of the Service Desk, this should have industry standard and enterprise scale features including but not limited to: Voice recording, recall and playback, call routing, customisable in accordance with Buyer priority IVR Performance reporting and heat mapping of peak contact volumes Pre-recorded message playback for Service announcements, Service interruptions or other key service information to End Users	**Must**
DSK.010	Service Management and Service Integration	**Service Desk**	The Supplier must ensure that all communications with the Buyer and all End User customers of the Service Desk must at all times be in the English language (covering all written or electronically captured and verbal communication). The Supplier must when communicating minimise technical language or terminology wherever possible to ensure ease of understanding by the End User	**Must**
DSK.011	Service Management and Service Integration	**Service Desk**	The Supplier should use the Buyer MyIT Service Portal to provide real time communications to End Users. This should include but is not limited to: Service disruption Operational changes New/updated Knowledge Articles	**Must**
DSK.012	Service Management and Service	**Service Desk**	The Supplier must adhere to the Buyer Incident Management process when managing incidents and associated contact with End Users.	**Must**
DSK.013	Service Management and Service Integration	**Service Desk**	The Supplier should implement (or operate the Buyers solution) a toolset approved by the Buyer for the remote access to and control of End Users Devices, to facilitate incident and support resolution. Access to an End Users Device must be with the express authorisation from the identified End User of the Device being taken over. All remote access sessions should be recorded for audit purposes including date / time of 'take over', length of time accessing users device, date / time of remote session finishing and the authorised user who assumed remote control.	**Should**
DSK.014	Service Management and Service Integration	**Service Desk**	The Supplier should cater for differing Persona types including but not limited to Standard Office Users Standard Field Users Assistive Technology Users VIP Users The Service Desk should recognise the different communication requirements that may exist with differing Persona types and use the most appropriate method for each individual. A differential priority may be assigned to these User types in agreement with the Buyer	**Should**
DSK.015	Service Management and Service Integration	**Service Desk**	The Supplier must resolve complaints in accordance with the Buyer's Complaint Management Process and in accordance with the Call Off Schedule 3 (Service Levels, Service Credits and Performance Monitoring).	**Must**
DSK.016	Service Management and Service Integration	**Service Desk**	The Supplier must integrate it's Service Desk operations with the Buyer's Service Management processes for the management and maintenance of all Service Requests, Service Issues and Incidents (including Major Incidents) during the Incident/Request response lifecycle. This includes preparation, detection and analysis, containment, eradication and recovery, and post-incident activity. This applies to both user and Supplier raised tickets.	**Must**
DSK.017	Service Management and Service Integration	**Service Desk**	The Supplier should provide Service management, performance and Service Experience reporting to support the optimal delivery of the Service. Ad-hoc additional reporting may be requested by the Buyer in addition to the above reporting requirements, which should be agreed with the Supplier.	**Should**
DSK.018	Service Management and Service Integration	**Service Desk**	The Supplier must ensure the Knowledge Management content that the Supplier is responsible for (in agreement with Buyer), is reviewed and updated to ensure content is accurate, relevant, fit for the purpose intended and aligned to current End User or EUS Service needs and requirements. Knowledge Article content must align to the Buyer Knowledge Management process. All Knowledge Articles that the Supplier is responsible for must be reviewed and updated for accuracy as identified by either party or at least annually.	**Must**

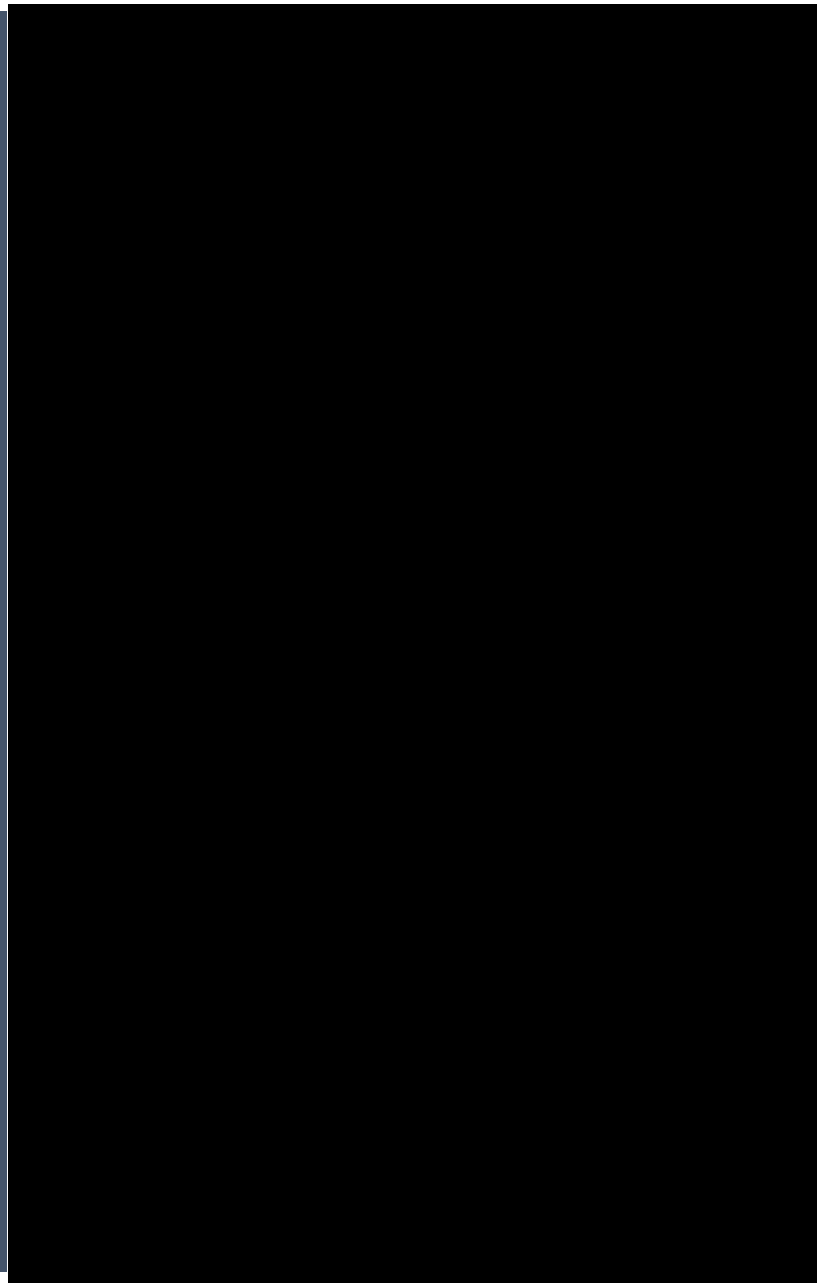


DSK.019	Service Management and Service Integration	**Service Desk**	The Supplier must create, test and publish Knowledge Articles with the aim of enhancing the effectiveness of the Service Desk as soon as the Supplier identifies that a Knowledge Article is required to address the issue identified. Knowledge Articles will provide concise targeted and tailored information to address specific issues, improve troubleshooting capabilities and support the Service Desk in delivering high quality and timely resolution of incidents.	**Must**
DSK.020	Service Management and Service Integration	**Service Desk**	The Supplier should align to the Buyer Service Readiness process for the on-boarding or off-boarding of Services.	**Should**
DSK.021	Service Management and Service Integration	**Service Desk**	The Supplier should as part of monthly reporting and governance propose to the Buyer opportunities and initiatives to improve the service to the End User. Continuous Improvement initiatives (where approved for implementation) are to be monitored and tracked for effectiveness.	**Should**
DSK.022	Service Management and Service Integration	**Service Desk**	The Supplier should propose methods of gathering and assessing the User experience (of the Suppliers service) and reporting on this via monthly governance forums. The user experience insight should form the basis for Continual Service Improvement Initiatives.	**Should**
DSK.023	Service Management and Service Integration	**Service Desk**	The Supplier should as part of the onboarding process ensure that all Service Desk agents attend familiarisation / training sessions to gain insight and understanding of the unique characteristics of the Defra organisation, its associated Arms Length Bodies and specialist areas (such as Labs) that are supported under this contract. The Supplier should ensure that its personnel working on the Buyer account maintain current awareness of Core Defra group respective business functions and services throughout the contract term.	**Should**
DSK.024	Service Management and Service Integration	**Service Desk**	The Supplier must propose methods and candidate opportunities to 'Shift Left' the focus whereby incidents are resolved (i.e. from Level 2 resolver teams to Service Desk to self help by User to eradication of the need). Shift Left identification must be included within the Suppliers Continual Service Improvement Initiatives and reported on monthly.	**Must**

BUYER REQUIREMENTS				BIDDER COMPLIANCE RESPONSE	
ID	Service Function	Requirement	MoSCoW	Fully Compliant Partially Compliant Non-Compliant	COMPLIANCE STATEMENT [MAX 100 Words]
SOC.001	**Security Operations Centre**	The Supplier must accept tickets from the DEFRA Security Operations Centre using the Authority's ITSM tool and investigate as per the agreed SLA.	**Must**	[redacted]	[redacted]
SOC.002	**Security Operations Centre**	The Buyer's SOC will monitor all endpoints via Defender for Endpoint, incidents raised as a result of Defender for Endpoint alerts may be passed to the supplier for investigation. The supplier must accept these tickets as per requirement SOC.001	**Must**		
SOC.003	**Security Operations Centre**	The Supplier must support requests for additional log data to support the Authority's cyber incident response process when required.	**Must**		
SOC.004	**Security Operations Centre**	Should the Supplier require the use of any subscriptions/resources in Defra's cloud tenancies (Azure/AWS, managed by the Cloud Centre of Excellence) in order to provide any aspect of their services, whether in production or pre-production, these will be protectively monitored by the Buyer SOC unless the Buyer explicitly requests the Supplier to carry out the protective monitoring or until such a time as the Buyer requires the Supplier to carry out the protective monitoring.	**Must**		
SOC.005	**Security Operations Centre**	The Supplier must attend regular 'collaboration' calls with the Buyer SOC to review tickets raised in the previous period and discuss any other pertinent operational matters.	**Must**		
SOC.006	**Security Operations Centre**	The Supplier must provide the Buyer SOC with a named Security Account Manager with whom the Buyer SOC can liaise on operational matters.	**Must**		
SOC.007	**Security Operations Centre**	The Supplier must attend an introductory 'scope of service' call with the Buyer SOC upon service commencement to explain the scope of the service and technology and hardware used. Further six monthly 'scope of service' calls must be held to update SOC on any technological changes.	**Must**		
SOC.008	**Security Operations Centre**	The Supplier shall upon instruction from the Buyer's SOC team representative, (in response to the discovery of a User account or Device that has had its security integrity compromised), disable the user account and device until investigations have been undertaken and the security compromise resolved. Requests for disabling of accounts can be made by the Buyer through the security incident management process.	**Must**		

BUYER REQUIREMENTS					BIDDER COMPLIANCE RESPONSE	
ID	Operational Area	Service Function	Requirement	MoSCoW	Fully Compliant Partially Compliant Non-Compliant	COMPLIANCE STATEMENT [MAX 100 Words]
SUS.001	Sustainability	Sustainability - General	Sustainable Procurement is addressed as a core part of the Buyer's commercial approach. We expect our stakeholders to share this approach, understand the relevant sustainability risks and opportunities, think innovatively to remove barriers, and work collaboratively to maximise sustainable outcomes. The supplier must support the Buyer in delivering its strategic priority outcomes by meeting and reporting on a set of robust Sustainability KPIs.	Must		[redacted]
SUS.002	Sustainability	Sustainability - General	The Supplier must reduce unsustainable impacts of services provided whilst enabling the Buyer to meet its environmental and net zero objectives. The service must be designed with industry best practice sustainability principles, delivering positive environmental outcomes and improving resilience.	Must		
SUS.003	Sustainability	Sustainability - General	The Supplier must ensure that the provision of the services support the Buyer's core deliverables in it's efforts to achieve and comply with: o Defra's Sustainable IT Strategy o Greening government: ICT and digital services strategy 2020 to 2025 o Greening Government Commitments 2021 to 2025 - GOV.UK (www.gov.uk)	Must		
SUS.004	Sustainability	Sustainability - General	The Supplier must agree to deliver the service in line with the Buyer's net zero targets and commitments, as follows: • The Department for Environment, Farming and Rural Affairs (core Government Department) has a target to reach net zero emissions by 2050 [as documented here https://www.gov.uk/government/publications/net-zero-strategy] • The Environment Agency has committed to reach net zero by 2030 [as documented here https://www.gov.uk/government/publications/environment-agency-reaching-net-zero]	Must		
SUS.005	Sustainability	Sustainability - General	The supplier must follow up the commitment made to becoming net zero with a road map and action plan, providing proven progress towards the goals. Seeking a carbon positive/net gain/net positive outcome through the services provided.	Must		
SUS.006	Sustainability	Sustainability - General	The Supplier must (when designing, implementing and delivering the Services) adopt the applicable elements of the UK Government's Technology Code of Practice as documented at https://www.gov.uk/service-manual/technology/code-of-practice.html	Must		
SUS.007	Sustainability	Sustainability - General	The Supplier must ensure that IT Assets shall as a minimum comply with Government Buying Standards(GBSs) at https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs where those standards exist for the asset type concerned e.g. laptops, desktops, workstations, scanners and printers.	Must		
SUS.008	Sustainability	Sustainability - General	The Supplier must follow a sound environmental management policy and should have ISO 14001 certification for its environmental management practices (or equivalents agreed with the Buyer), ensuring that any Goods and the Services are procured, produced, packaged, delivered, and are capable of being used and ultimately disposed of in ways appropriate to such standard.	Must		
SUS.009	Sustainability	Sustainability - General	The Supplier must report and measure the carbon footprint (up to and including scope 3) and environmental impacts specifically pertaining the service consumed by the Buyer on at least an annual basis over the duration of the contract.	Must		
SUS.010	Sustainability	Sustainability - General	The Supplier must provide annual progress reports to demonstrate improvements around carbon reduction, data efficiencies, supply chain data on carbon, environmental impacts, materials, chemicals, and wider business responsibilities and evidence of governance to support the delivery of progress. The supplier must provide reporting for management and awareness of resilience from climate and ecological breakdown of the services provided.	Must		
SUS.011	Sustainability	Sustainability - General	The Supplier must comply with all relevant obligations under the Waste Electrical and Electronic Equipment Regulations 2013 in compliance with Directive 2002/96/EC and subsequent replacements (including those in compliance with Directive 2012/19/EU).	Must		
SUS.012	Sustainability	Sustainability - General	The Supplier should comply with packaging requirements set out at Packaging (Essential Requirements) Regulations 2015 (as amended) and Producer Responsibility Obligations (Packaging Waste) Regulations 2007 (as amended)	Should		
SUS.013	Sustainability	Sustainability - General	The Supplier must support the Buyer to deliver 0% to landfill with an annual increase in reuse and materials recycled through the provision of any service.	Must		
SUS.014	Sustainability	Sustainability - General	The Supplier should use reasonable endeavours to avoid the use of packaging, paper and card in executing the Contract and where unavoidable ensure that any packaging, paper or card deployed in the performance of the Services (for example in deliveries, training materials, operating manuals and guides) should consist of 100% recyled materials or re usable or recyclable packaging. Where possible any packaging that cannot be reused or recycled should be substituted with that which can. Single use plastic packaging for deliveries should be avoided. Paper/card should not be bleached with chlorine.	Should		
SUS.015	Sustainability	Sustainability - General	In supporting the Buyer to reduce its supply chain's greenhouse gas emissions, the Supplier must avoid fuel emissions in transporting goods and in Supplier Staff travel to Buyer Premises for staff engaged in delivering Services wherever possible, and without exclusion, by: using e-conferencing services, using logistics to rationalise journeys and minimise miles travelled in the transportation of goods to Buyer Premises, provide online training to minimise travel and use electric/hybrid vehicles or the rail service rather than petrol or diesel powered vehicles.	Must		
SUS.016	Sustainability	Sustainability - General	The Supplier must explain the sustainability requirements to all Supplier Staff and sub-contractors involved in the performance of the Supplier's obligations under this Contract. The Supplier shall ensure that equivalent obligations to those contained in this Contract are included in any contract with any sub-contractor that is connected to this Contract. The Supplier must ensure that that all Supplier and sub-contractor Staff, regardless of role: - are made aware of the requirements of this Schedule; - are trained and competent to deliver the requirements of this Schedule appropriate to their role; and - in the case of Supplier Staff, receive training on the contents of this Schedule: o as part of their induction when joining the Supplier Staff; and o at least annually thereafter. The Supplier shall ensure that equivalent obligations to those contained in this Contract are included in any contract with any sub-contractor that is connected to this Contract The Supplier acknowledges that sub-contractors include: - those providing services that indirectly support the provision of the Services; and - any organisation that provides the Premises or any facilities or services on the Premises.	Must		
SUS.017	Sustainability	Sustainability - General	The Supplier should participate in communities of practice formed by the Buyer in order to share good practice and support the improvement of sustainability performance.	Should		
SUS.018	Sustainability	Sustainability - Hardware	The Supplier must follow the Waste Hierarchy (meaning the Guidance on applying the Waste Hierarchy published by the Buyer pursuant to regulation 15(1) of the Waste (England and Wales) Regulations 2011) in disposing of assets (on The Buyer's estate or off-site) no longer required for delivery of the Service.	Must		

SUS.019	**Sustainability**	Sustainability - Hardware	The Supplier must have circular ICT policies and strategies, and products are routinely designed for durability, ease of maintenance and recycling. Problematic materials and substances have, or are being, phased out of use. A disposal plan must be submitted to outline how assets pertaining to the Service (on The Buyer's estate or off-site) will be managed at end of life and/or for assets being decomissioned as part of the service provide.	**Must**
SUS.020	**Sustainability**	Sustainability - Hardware	The Supplier must ensure that the use and disposal of any hazardous substances used in manufacturing assets and consumables (being paper, toner, and any replaceable components of assets deployed including batteries, disk drives, printer drums) is in compliance with The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012.	**Must**
SUS.021		Sustainability - Hardware	The Supplier must comply with UK requirements of producers to handle disposal of batteries they place in appliances provided as part of the Service. https://www.gov.uk/guidance/waste-batteries-producer-responsibility	**Must**
SUS.022	**Sustainability**	Sustainability - Hardware	The Supplier must ensure and demonstrate the new assets deployed for the service (on The Buyer's estate or off-site) have minimised the use of non-renewables, rare earth metals and critical raw materials in their construction and maximised the use of recycled/recovered materials and materials from renewable sources.	**Must**
SUS.023	**Sustainability**	Sustainability - Hardware	The Supplier must ensure and demonstrate how in the manufacture of assets required for the delivery of the Service, it has, wherever possible, utilised power from renewable energy sources and minimised water consumption.	**Must**
SUS.024	**Sustainability**	Sustainability - Hardware	For asset types where there are no Government Buying Standards or Green Public Procurement criteria available, the Supplier must ensure that the models of asset deployed (pertaining to the Service deployed on Defra estate or off-site) have Energy Star (using ECMA or equivalent declarations agreed with the Buyer), and comply with EPEAT or equivalent schemes for sustainable management of resources and energy over the asset lifecycle.	**Must**
SUS.025	**Sustainability**	Sustainability - Services	The Supplier must ensure services will be operated in such a way as to minimise energy consumption, both directly in the service assets (computers, monitors etc), and indirectly in the support infrastructure (buildings, cooling, lighting, water supply) and operational travel/transport needs.	**Must**
SUS.026	**Sustainability**	Social Value	The Supplier must ensure opportunities to recruit and employ apprentices attract and are inclusive to candidates from all backgrounds including those who face barriers to employment (e.g. those from deprived or underrepresented backgrounds, ex-military, ex-offenders). The Supplier must report to the Buyer the numbers of apprentices employed and the wider skills training provided, during the delivery of the service.	**Must**
SUS.027	**Sustainability**	Social Value	The Supplier must demostrate regularly how they are delivering their social value plan as set out in their response and demonstrate evidence that the outcomes are delivered through the following: - The Supplier must deliver their social value commitments set out within their social value plan. This includes providing regular updates to the Buyer on the approach taken, progress against the action plan and details of the outcomes/value delivered (quantity and quality) - The Service Provider, as an organisation, addresses workforce imbalance by supporting disadvantaged, underrepresented and minority groups into employment (including apprenticeships and other training schemes) throughout the Service Period. - The Service Provider will support the Client in highlighting opportunities to provide wider social, economic, or environmental benefits to local and/or national communities though the delivery of the contract. The Service Provider will provide details to the Client of the approach taken, progress made and benefits delivered.	**Must**
SUS.028	**Sustainability**	Social Value - Wellbeing	The Supplier shall: make a commitment to supporting and investing in health and wellbeing, including physical and mental health, in the contract workforce; report on percentage (%) staff survey improvement of work satisfaction with year-on-year improvement for staff in the annual sustainability report; and report on the percentage (%) of companies in the supply chain under the contract to have implemented measures to improve health and wellbeing of employees, including the Mental Health at Work Commitment and Thriving at Work.	**Must**
SUS.029	**Sustainability**	Social Risks - Supply Chain	The Supplier must work to improve transparency in their supply chain by mapping the highest risk goods and services. For agreed high risk areas the Buyer expects full transparency of the supply chain e.g. raw material extraction through to use at site. The Supplier must work with the Buyer to transpose the supply chain data into geographic risk data and overlay with key data such as the Global Slavery Index, Water Stress and Climate Change. This will help to understand the risks and look at reducing them.	**Must**
SUS.030	**Sustainability**	Social Value - Supplier Diversity	When sub-contracting, the Supplier must ensure that supply chain opportunities are inclusive and accessible to Small and Medium Enterprises (SMEs) and Voluntary Community and Social Enterprise (VCSE) organisations, Mutuals, new businesses and entrepreneurs and other underrepresented business groups. The Supplier must identify barriers for these organisations and will work actively to remove them, ensuring equal opportunities to compete. The Supplier will report on this annually. The Contracts Finder website can be used to help advertise any subcontracting opportunities outside the established supply chain. Other routes advertising to SMEs, VCSE organisations and other underrepresented business groups should be sought to highlight opportunities and encourage a diverse and inclusive supply base.	**Must**
SUS.031	**Sustainability**	Social Risks - Human Rights	The Buyer is committed to ensuring that workers employed within its supply chains are treated fairly, humanely, and equitably. The Buyer requires the Supplier to share this commitment and use reasonable and proportionate endeavors to identify any areas of risk associated with this Service and its operations. The Supplier must ensure that its sub-contractors and other organisations in its supply chain: (a)respect the right of their workers to freely and voluntarily establish and join groups for the promotion and defence of their occupational interests; (b)provide effective and good faith recognition of the right to collective bargaining of their workers; (c)not engage their workers in terms of slavery, servitude, or forced or compulsory labour; (d)not use child labour; (e)not discriminate in the engagement of their workers on the basis of the Protected Characteristics.	**Must**
SUS.032	**Sustainability**	Social Risks - Human Rights - Modern Slavery	The Supplier must, and must ensure that its sub-contractors and other members of its supply chain, comply with section 54 of the of the Modern Slavery Act 2015, where that provision applies to any particular organisation.	**Must**
SUS.033	**Sustainability**	Social Risks - Human Rights - Modern Slavery	The Supplier must have completed the Modern Slavery Assessment Tool (MSAT) as per the Tech Services 3 framework prior to Award and develop a continuous improvement plan progress to be shared with the Buyer to be agreed with the Buyer and improvement evidenced.	**Must**
SUS.034	**Sustainability**	Social Risks - Human Rights - Modern Slavery	The Supplier must re-visit their assessment regularly and when there are key changes that could change their risk of modern slavery. The Supplier must share the action plan from the assessment with the Buyer and proactively work to address the actions identified regularly reporting on continuous improvement against the actions.	**Must**
SUS.035	**Sustainability**	Social Risks - Human Rights - Modern Slavery	Within 90 days from the commencement of the service the Supplier will provide a summary of the risks of modern slavery relevant to the service along with steps that will be taken to address them and work to improve supply chain transparency. The Supplier must provide an annual due diligence report to demonstrate progress against mitigating modern slavery risk relavant to the contract.	**Must**



SUS.036	**Sustainability**	Social Risks - Human Rights - Modern Slavery	The Supplier will work with the Buyer to identify and mitigate the risk of modern slavery, human trafficking, forced and bonded labour and human rights violations in its supply chain. The Supplier will work to improve transparency in their supply chain by mapping the highest risk goods, services and/or works within [add in reasonable timeframe e.g. 1 year]. The Supplier shall implement a system of training for its employees and sub-contracted staff to ensure awareness of modern slavery risks, legislation and to understand its relevance to their role. This will include how to recognise the signs of modern slavery and report it, the training must be available in a format staff can understand. This will be implemented in Year 1 of the contract. A copy of the training and records will be made available to the Buyer on request. Within 90 days for the Service commencing, The Supplier shall provide a Social Audit plan to be carried out by appropriately trained auditors on how they will investigate potential indicators of modern slavery and are familiar with issues in the specific regions impacted which clearly demonstrate the Suppliers commitment to undertake third party audits so that: - they utilise a baseline from a prior risk assessment has been carried out which gives assessors a clear overview of the types of vulnerable workers who may be present and some of the drivers of modern slavery risk in the region or sector. - the focus on areas of investigation and questions should be adjusted to focus on these previous findings. - encompass a 'do-no-harm' approach in in the first instance and safeguards are put in place to ensure that actions by an assessor or investigator do not put vulnerable workers at greater risk, nor compromise the ability to conduct further investigation by competent authorities if criminal abuse and exploitation is suspected. - focus primarily on understanding worker perspectives of the issues, via interviews carried out in a confidential setting, in the workers' own language and triangulating this information with evidence submitted by management. A sample size of 15-20% of the migrant workforce is recommended.	**Must**
SUS.037	**Sustainability**	Social Risks - Human Rights	The Supplier must minimise the use of Conflict Minerals in sourcing materials for the manufacture of the assets deployed in delivering the Service in accordance with UK government guidance set out at https://www.gov.uk/guidance/conflict-minerals.	**Must**
SUS.038	**Sustainability**	Social Risks - Human Rights	The Supplier must use reasonable and proportionate endeavours ensure that workers employed within its supply chain are treated fairly, humanely, and equitably.	**Must**
SUS.039	**Sustainability**	Social Risks - Equality, Diversity & Inclusion	The Buyer is striving to create a diverse and inclusive working environment where every individual has equality of opportunity to progress and to apply their unique insights to making the UK a great place for living. The Supplier is expected to respect this commitment in all dealings with Buyer staff and service users. The Supplier will comply with any Equality, Diversity & Inclusion (EDI) clauses set out in the contract. Including reporting any incidents relevant to the contract to the Buyer immediately. The Supplier must; - support Buyer to achieve its Public Sector Equality Duty as defined by the Equality Act 2010, and to support delivery of the Buyer's Equality & Diversity Strategy. - meet the standards set out in the Government's Supplier Code of Conduct. - have an approach in place to identify any equality impacts (both positive and negative) in the delivery of this contract, and to mitigate any negative impacts and realise the opportunities, including (but not limited to): o how solutions are accessible to disabled customers and staff (including those with physical disabilities, sensory impairments, and neurodiverse conditions) o how will you ensure that language used is inclusive of all protected groups (as defined by the Equality Act) - monitor, at every stage of delivery of the contract, whether the solutions developed, or services delivered present any barriers to any of the protected groups and ensure that any such barriers will be addressed. - ensure that staff (including sub-contractors) who will be working on this contract): o understand the Equality Diversity and Inclusion issues relevant to their roles and how to address them. o are familiar with best practice in relation to accessibility and inclusive customer service - the Supplier will ensure that processes are in place to gather feedback from the Buyer and from end users, including feedback on EDI issues, and ensure that action plans are put in place to address any feedback received and progress regularly monitored. - the Supplier will provide evidence of providing the Buyer's EDI guidance by supporting disadvantaged	**Must**
SUS.040	**Sustainability**	Social Risks - Equality, Diversity & Inclusion	The Supplier should, as an organisation, addresses workforce imbalance by supporting disadvantaged, underrepresented and minority groups into employment (including apprenticeships and other training schemes) throughout the Service Period.	**Should**
SUS.041	**Sustainability**	Social Risks - Whistleblowing	The Supplier must, and must ensure that it's sub-contractors, have in place, promote and properly implement policies designed to allow members of staff to: - raise concerns about any failure of the Supplier or the sub-contractor to: o comply with the provisions of this Contract o comply with the Law; and o raise a grievance where that person considers the Supplier or sub-contractor (as appropriate) has not complied with any of the requirements relating to it's staff in this Schedule. The Supplier shall: - insert the following wording into its whistleblowing policy and communicate to all it's staff that engaged in delivering the Services in a format they can understand: "If you feel unable to raise your concern internally and it relates to work being carried out for which the beneficiary (through a contractual chain or otherwise) is Defra group, please email whistleblowing@Defra.gov.uk." - ensure that their sub-contractors and their Staff are aware that they may raise concerns directly to the Buyer under its whistleblowing policy. - The Supplier must not, and must ensure that sub-contractors do not, retaliate against any member of Staff who: o raises a grievance under any policy referred to in paragraph 8.1; or o raises a concern internally or with the Buyer under the Supplier's whistleblowing policy	**Must**
SUS.042	**Sustainability**	Enviromental Risk - Climate Change and Adaption	The Supplier shall ensure that it and its sub-contractors: - demonstrate an understanding of the risks to the Service relating to extreme weather (such as flooding and extreme temperatures), a changing average climate and resource scarcity. This should include the risks associated with the supply chain. The Supplier will provide an annual assessment to the Authority of those risks and any mitigations being employed as part of its Sustainable Operations report; and - ensure that any identified risks are covered off in business continuity plans developed in accordance with continuity planning.	**Must**

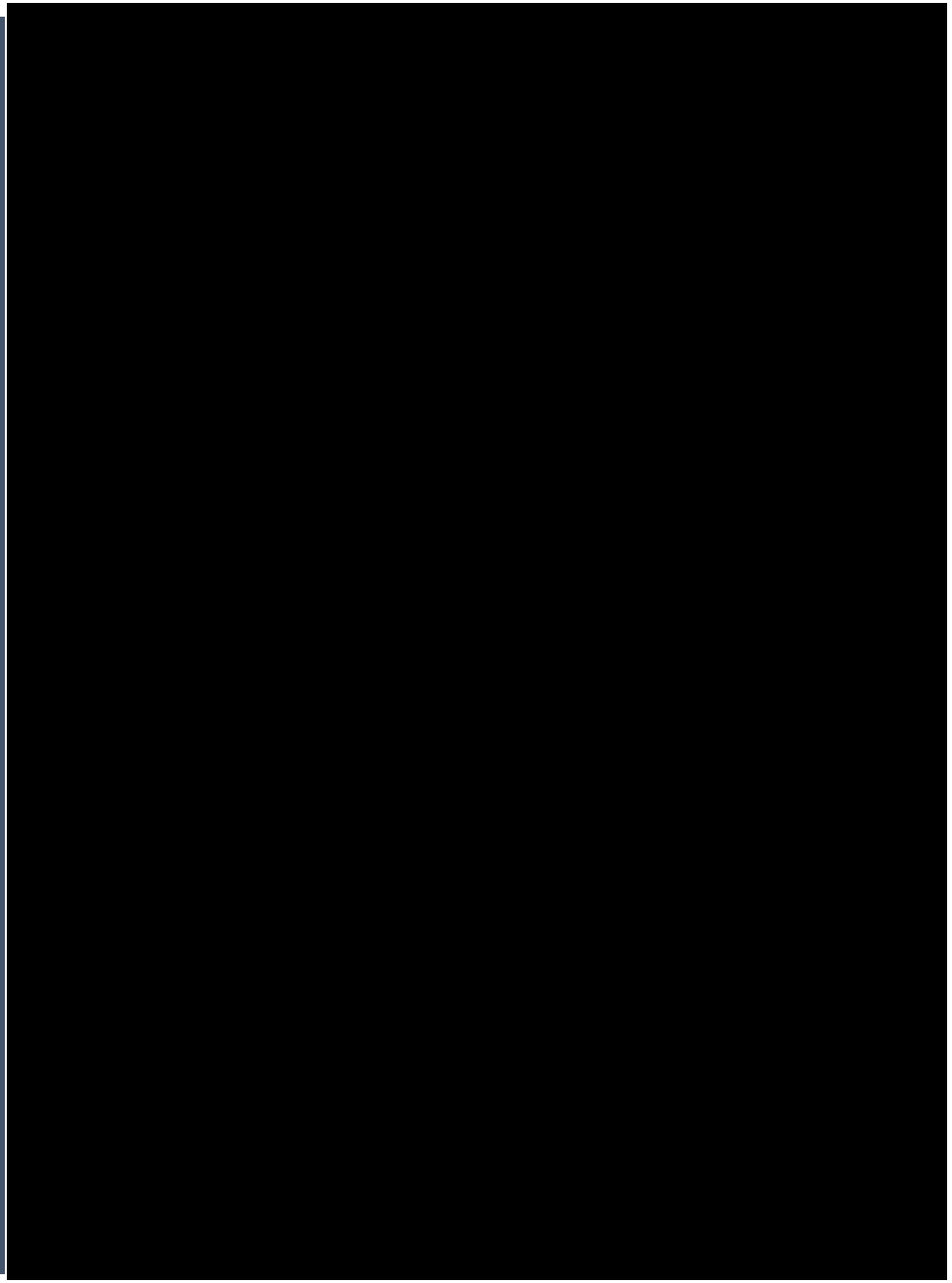
[redacted]

BUYER REQUIREMENTS					BIDDER COMPLIANCE RESPONSE	
ID	Operational Area	Service Function	Requirement	MoSCoW	Fully Compliant Partially Compliant Non-Compliant	COMPLIANCE STATEMENT [MAX 100 Words]
CMR.001	Connectivity	**IT Comms Room**	The Supplier shall arrange with the Buyer contacts provided for site for any access requirements. Where there are project requirements, which may require longer periods of access to a location, the Supplier shall liaise with Buyer project counterparts in the first instance to confirm requirements prior to contacting site to ensure appropriate access and escort. For sites that have been identified as requiring SC clearance by the Buyer, the Supplier shall provide resources with appropriate clearance and shall arrange with the Buyer contacts for a full time escort. This includes the Project providing escort duties if required.	**Must**	[redacted]	
CMR.002	Connectivity	**IT Comms Room**	The Supplier shall comply with any site specific health and safety policies, including provision of any necessary documentation in advance (e.g. RAMS - Risk and Method Statements) to the local Facilities team for any work to be undertaken in comms rooms and/ or within the Authorities property demise/ areas of responsibility.	**Must**		
CMR.003	Connectivity	**IT Comms Room**	The Supplier shall comply with specific Comms Room H&S where these are not already covered by site H&S policies - "IT guidance for DDTS Suppliers PBT Facilities Estates v2.12" and any subsequent updates	**Must**		
CMR.004	Connectivity	**IT Comms Room**	The Supplier is responsible for surveying a Comms Room for any new requirements, and must engage the Buyer for any new infrastructure required in a Comms Room as a result either under a project or BAU activity.	**Must**		
CMR.005	Connectivity	**IT Comms Room**	The Supplier must remove any decommissioned kit, including any patch cables, from a comms room within 20 working days of service being ceased or replaced. The Buyer reserves the right to charge the Supplier for storage if kit is not removed, or the Buyer will dispose of kit and charge the Supplier for doing so.	**Must**		
CMR.006	Not Used	**Not Used**	Not Used	**Must**		
CMR.007	Connectivity	**IT Comms Room**	The Supplier(s) must ensure all local backup media still in use is transferred to the cloud. i.e. all backups to become electronic and a 'cloud first' approach. Where backup media is currently used in a Comms Room, the Supplier shall ensure backups are taken at the necessary frequency and are responsible for storing the media securely - not at Buyer premises - and for ensuring backups can be restored as needed. For new services, no backup media at site is to be used as all backups shall be electronically with a 'cloud first' policy adopted.	**Must**		
CMR.008	Connectivity	**IT Comms Room**	The Supplier must inform local Facilities the same day and the Service Manager within 1 working day, of any possible security or H&S issues they identify within the Comms room. The Supplier must ensure any work they undertake in a comms room does not introduce a H&S and/or security risk.	**Must**		
CMR.009	Connectivity	**IT Comms Room**	The Supplier must clear up after any works and dispose of any rubbish generated by their work sustainably in adherence to waste packing and WEEE requirements.	**Must**		

CMR.010	Connectivity	**IT Comms Room**	The Supplier must engage with the relevant Buyer Facilities team before undertaking any work that includes penetrating the building fabric, and confirm what work is required to make good any damage before work starts. Any costs associated with this shall be inclusive in the delivery of the works. The Buyer retains the right to charge the Supplier for remedial work if the remedial work by the Supplier/ project is not accepted by the Buyer's Facilities team.	**Must**	[redacted]
CMR.011	Connectivity	**IT Comms Room**	The Supplier must follow the requirements in the "IT guidance for DDTS Suppliers PBT Facilities Estates v2.12" and any subsequent updates for undertaking work at a Defra Group site, unless specified differently in a contract e.g. network procurement, hosting, end user.	**Must**	

BUYER REQUIREMENTS					BIDDER COMPLIANCE RESPONSE	
ID	EUS Category	Service Function	Requirement	MoSCoW	Fully Compliant Partially Compliant	COMPLIANCE STATEMENT [MAX 100 Words]
EUS.001	Tech Bar	**End User Services**	The Supplier must, provide on-site tech bar support at the Buyer Defined Locations which must include but is not limited to: (a) face to face, floor walkers and deskside support; (b) drop in surgeries(walk up support) / tech bars to support End Users (including Assistive Technology Users); (c) maintain equipment / peripherals that can be provided to End Users; (d) support to End Users who use Assistive Technology; (e) offer bookable appointments for 1:1 support / advice on End User related IT issues (f) video conferencing and audio visual collaboration conferencing support (g) maintenance and support of smart lockers	**Must**		
EUS.002	Tech Bar	**End User Services**	The Supplier should demonstrate flexibility to increase or reduce tech bar services within the Buyer Defined Locations upon the request of the Buyer	**Should**		
EUS.003	EUS Asset Related	**End User Services**	1. The Supplier must ensure that all Devices are sourced from Tier 1 vendors either directly from the Original Equipment Manufacturer (OEM), or via a distribution channel who conforms to the UK Government Security Standards in accordance with Buyers Minimim Device Specification as set out in the Device Strategy. 2. The Supplier must, provide the ability to forward forecast stock levels required to meet demand based on historical data and other leading indicators. 3. The Supplier must, as agreed with the Buyer in monthly service review meetings, maintain defined stock levels for the in-scope hardware. The Supplier is responsible for the accuracy and insight of the forcasting data and the management of the supply chain and logistics around stock reordering and stockholding. This responsibility shall include the provision and management of spares whether recycled/reuse or new spares. 4. The Supplier must, proactively identify inactive assets and coordinate the removal or reallocation of such assets with the guidance of the Buyer. 5. The Supplier must manage the stock in accordance with this Contract, where stock needs to be replenished the Supplier will advise the Buyer and include suggested products that meet the minimum specification. The Buyer will instruct the Supplier to procure on its behalf the agreed replacement products and volumes thereof. 6. The Supplier must, ensure that all of the End User equipment returned to or from the pool of spare stock is tracked throughout its lifecycle. 7. The Supplier must, provide to the Buyer a monthly report for all items that have been removed from the asset register that are beyond economic repair and seek approval from the Buyer to be decommissioned. 8. The Supplier must, in agreement with the Buyer, define and deliver a process for ensuring scrappage, data deletion and decommissioning of all End User equipment, and provide certification of completion.	**Must**		
EUS.004	EUS Asset Related	**End User Services**	The Supplier must, provide all logistical services (for example, provisioning site preparation etc.) associated with the movement of the equipment or software from Third Party Suppliers to Supplier or Buyer designated locations. The Supplier must, verify that End User equipment is stored in a secure area and are not subject to extreme heat, cold, dampness, dirt in accordance with manufacturers environmental storage recommendations. The Supplier must, ensure all assets: (a) contain a visible asset identifier, which is robust and visible to the End User which matches the digital identifier; (b) are stored and recorded within the CMDB before the asset is used; and (e) are updated to ensure that the asset and configuration record is current. The Supplier must, ensure when any asset loss or theft has been identified inform the Buyer immediately outlining the: (a) asset details; (b) value; (c) user information; (d) any data loss or potential risk; (e) the circumstances and investigation; and (f) where applicable and agreed with the Buyer invoke remote wipe as per the Security standards.	**Must**		

EUS.005	EUS Asset Related	**End User Services**	"The Supplier must, as agreed with the Buyer, provide an asset report outlining but not limited to the following: (a) utilisation of assets, including but not limited to the End User Devices is allocated to; (b) asset age and end of life (EOL) status; (c) current level of stock required to meet SLA and Operational Business Change needs; (d) details of consumables e.g. cables and PSU for branch devices; (e) maintenance / reporting on PAT re-test status; (f) Last logon information;and (g) Device patch / update status (including firmware versions). The Supplier must, for each Service Period, produce a disposal report detailing assets disposed of, last user and confirmation of secure data destruction in accordance with Buyer security policies and processes. The Supplier must, sample check, no more than monthly, all stock inventory to ensure quality whilst held in the Supplier's secure storage. The Supplier must, provide the Buyer with a report, no more than monthly or as required by the Buyer, detailing the Supplier's stock management information."	**Must**
EUS.007	Catalogue and Request	**End User Services**	The Supplier should ensure that it has stock of Devices sufficient to cover the average monthly order volumes as agreed with the Buyer.	**Should**
EUS.008	Device Management and Control	**End User Services**	Prior to issuing a Device to an User, the Supplier must ensure that all Devices are issued in accordance with the Buyer's Service, Asset and Configuration Management policies and associated process documents. The policies and processes will be reviewed regularly and updates will be communicated to the Supplier who will enact any required changes within an agreed reasonable time. This will include, but not limited to, the following; -registered to the Buyer within the appropriate device management tool (for example Apple Business Manager for Apple devices); -enrolled in the Buyer's InTune production environment which will provide performance data to measure Device effectiveness -enrolled in MyIT (ServiceNow) to enable the Device, sofytware and related services to be tracked throughout the life of the Device The Supplier will utilise these Buyer tools to provide the full lifecycle management of the Device including but not limited to deployment, management, repair, returns and disposals in accordance with the Buyer's Service Asset and Configuration Management policies and associated process documents.	**Must**
EUS.009	Device Management and Control	**End User Services**	The Supplier must ensure that all Devices are appropriately restricted via the correct Role Based Access Controls assigned via correct InTune policy assignment.	**Must**
EUS.010	EUS Asset Related	**End User Services**	The Supplier must provide, manage, support and monitor all End User Devices and Peripheral equipment throughout the lifecycle of all hardware equipment. This includes from onboarding users devices to offboarding.	**Must**
EUS.011	EUS Asset Related	**End User Services**	End User Devices must be delivered to the end user in ready-to-use condition and in compliance with the Buyer's Hardware Asset Management Policy.	**Must**
EUS.012	Catalogue and Request	**End User Services**	The Supplier must ensure Devices, Peripherals, Consumables and approved software will be made available to order through the Buyer Service Catalogue. Fulfilment of Catalogue requests must be completed within the Service Levels agreed.	**Must**
EUS.013	Catalogue and Request	**End User Services**	The Supplier should provide a selection of Devices, Peripherals and Software (as specified by the Buyer) designed for different user persona types. This allows the choice of device and peripherals that are tailored to the Buyer's standardised user persona types and specific to job profiles and requirements. Persona types including but not limited to Standard Office Users Standard Field Users Assistive Technology Users VIP Users	**Should**
EUS.014	Catalogue and Request	**End User Services**	The Supplier must ensure that all items ordered by the Service Catalogue are configured in a ready to use condition, and where possible delivered in a single package. Where this is not possible the number of packages sent must be minimised to avoid excess transport and packaging impact.	**Must**
EUS.015	Device Management and Control	**End User Services**	Using performance monitoring tools, the Supplier must provide a service that ensures Devices are continuously and proactively monitored throughout it's lifecycle to allow the Supplier to pre-emptively predict Device performance, health, and any detrimental impact that the Devices performance may have on the User before it becomes a service impacting issue. Any foreseeable impact, issues or incidents predicted by the Supplier are to be proactively resolved by the Supplier. The Supplier must maintain the Buyer's preferred choice of performance based refresh model as set out in DEX.002 and DEX.003.	**Must**
EUS.016	EUS Services & Support	**End User Services**	The Supplier must obtain approval from the Buyer for any deviation in specification from the Defra Device Strategy prior to being provisioned to End Users.	**Must**
EUS.017	EUS Services & Support	**End User Services**	The Supplier should support all End Users to ensure that any specialist hardware or scientific equipment needed for the End Users to perform their day to day role is configured and functioning as intended on their End User Devices (including but not exclusively port connection and configuration, access, software or driver install).	**Should**



EUS.018	EUS Services & Support	**End User Services**	The Supplier must ensure that all End User Services are integrated with the Buyer identity solution to enable Single Sign On save for where exceptions have been formally agreed in writing between Supplier and Buyer.	**Must**
EUS.019	EUS Services & Support	**End User Services**	The Supplier must support the self service capability for End Users to reset their Device Windows password via Windows login and a secure web interface	**Must**
EUS.020	EUS Services & Support	**End User Services**	The Supplier must support the Buyer's multi-factor authentication for applications and services designated by the Buyer.	**Must**
EUS.021	EUS Services & Support	**End User Services**	The Supplier must operate its Services with access delegated from the Buyer as part of Role Based Access Control.	**Must**
EUS.022	EUS Services & Support	**End User Services**	The Supplier must ensure all hardware that goes into the containment labs is incinerated in conformity with the Buyer's process and procedure when they reach end of life, as per the Buyer Hardware and Asset Management Policy.	**Must**
EUS.023	EUS Asset Related	**End User Services**	The Supplier must ensure that the functionality and suitability of all Buyer Devices is known at all times throughout the device lifecycle. Functionality and suitability should include by way of example, battery life, screen, ports, keyboard, hard drive, overheating/cooling and network connectivity. The Supplier must provide reports on a monthly basis as to Device functionality and suitability. The Supplier must provide within the monthly report the status of the disposal routes for devices and peripherals, following categories of the waste hierarchy and in line with the Buyer Disposal Policy. The reports for disposed of IT assets should contain the minimum data sets as identified by the Buyer (e.g. Asset tags / serial numbers) for the updating of asset management toolsets and databases.	**Must**
EUS.024	Smart Lockers	**End User Services**	The Supplier will provide continued and ongoing support, management and operation of all existing Buyer lockers at the agreed Buyer locations.	**Must**
EUS.025	EUS Services & Support	**End User Services**	The Supplier should upon request from the Buyer provide Devices and Peripherals to the End User (based upon their Persona and use case). This service should be available at Users home address, Buyer Premises and installed Locker locations.	**Should**
EUS.026	EUS Asset Related	**End User Services**	The Supplier must either be, or sub-contract to an authorised certified repairer so that they can repair and re-issue Smart Devices and End User Devices.	**Must**
EUS.027	EUS Asset Related	**End User Services**	The Supplier must provide a service for the repair and refurbishment of Devices to the performance standards agreed with the Buyer. The Supplier must arrange a replacement for a Device that requires repair to minimise the impact on the End User of having a defective Device. Repaired Devices will be returned cleaned and sanitised state to the Device stock holding for future usage. Devices that are Beyond Economic Repair will be disposed of in line with the Buyer Disposal policy.	**Must**
EUS.028	EUS Asset Related	**End User Services**	The Supplier should provide channels to donate unneeded devices to beneficiaries as specified by the Buyer, including but not limited to charities.	**Should**
EUS.029	EUS Asset Related	**End User Services**	The Supplier should provide innovation opportunities for repair, recycling and re-selling, which support the principles of the circular economy.	**Should**
EUS.030	Catalogue and Request	**End User Services**	The Supplier must provide proactive, timely and accurate communications to End Users on the delivery of equipment, via SMS, email and Buyers ITSM Tool, which at the Commencement Date is ServiceNow.	**Must**
EUS.031	Device Management and Control	**End User Services**	The Supplier must manage and support a range of Devices, including Windows devices and non-Windows devices (e.g. Apple Macbooks).	**Must**
EUS.032	EUS Asset Related	**End User Services**	The Supplier should provide regular status updates (at least when the status changes) on the Buyer End User devices throughout the device lifecycle, from ordering, transporting, to return/disposal.	**Should**
EUS.033	EUS Asset Related	**End User Services**	The Supplier must adhere to the Defra Device Strategy and Minimum Device Specifications.	**Must**
EUS.034	Device Management and Control	**End User Services**	The Supplier should configure Devices to the highest efficiency settings available as default (e.g. Low screen brightness, hibernation mode, wi-fi connection over cellular connection), including the ability for end user to configure their devices within limits.	**Should**
EUS.035	EUS Services & Support	**End User Services**	The Supplier must maintain and support Microsoft Teams desk phone devices to the agreed performance metrics in the Buyer's environment.	**Must**
EUS.036	EUS Asset Related	**End User Services**	Where agreed with the Buyer, the Supplier should provide, maintain and support (including configuration) principles of just-in-time shipping of Buyer End User Devices direct from the Supplier's distribution partners to End Users at an approved location that the End User specifies. The Buyer wishes to avoid where possible excessive stock holdings and multiple handling considerations in line with modern management and sustainability principles.	**Should**
EUS.037	Smart Lockers	**End User Services**	The Supplier must procure on behalf of the Buyer (when requested) further smart lockers in addition to the current lockers available within the Buyer's estate, at the agreed Buyer locations. The Supplier must include support and maintenance of all lockers to a standard agreed with the Buyer until the end of Term. The specification of the lockers (overall size, number of locker bays and their capacity) to be agreed with the Buyer.	**Must**
EUS.038	Smart Lockers	**End User Services**	The Supplier will integrate the lockers into the buyer's ITSM Tool (ServiceNow) using open API's, where this does not require the creation of any customisations. The Supplier will update device location information and device assignment within the Buyer's ITSM CMDB (ServiceNow).	**Must**
EUS.039	Smart Lockers	**End User Services**	The Supplier must carry out device/peripheral and inventory management of the smart lockers, with device/peripheral traceability, sufficiently stocked, tracking of distribution and visit the smart locker locations as required to meet the Request Fulfilment SLAs and asset management responsibilities.	**Must**
EUS.040	Smart Lockers	**End User Services**	The Supplier will provide End Users with a unique authenticated code that allows them to either collect a device or peripheral from a locker or return equipment to a locker, these codes will be integrated into the buyer's ITSM Tool ticketing solution (ServiceNow).	**Must**

[redacted]

EUS.041	Smart Lockers	**End User Services**	The Supplier should provide insights and reporting on the smart lockers usage and maintenance as agreed with the Buyer. The Supplier will respond to alerts and notifications to ensure the lockers meet the agreed perfomance metrics.	**Should**
EUS.042	Smart Lockers	**End User Services**	The Supplier must take a proactive approach in utilising market insights to innovate and improve in agreement with the Buyer, all services including the smart locker service, thereby enhancing the Buyer's employee and customer experience.	**Must**
EUS.043	Catalogue and Request	**End User Services**	The Supplier must meet the Service Levels for managing and replacing lost/stolen Buyer End User Devices in line with the Buyer security policies and within the timeframes defined in the performance metrics agreed with the Buyer.	**Must**
EUS.044	Catalogue and Request	**End User Services**	The Supplier must meet the End User Device Configuration and deployment performance as agreed with the Buyer as set out in [SMR 075].	**Must**
EUS.045	EUS Security	**End User Services**	The Supplier must ensure endpoint security management is configured and operating in accordance with the Buyer End User Device Security Policy.	**Must**
EUS.046	EUS Services & Support	**End User Services**	The Supplier should support using all reasonable endeavours basis any devices that are operating on the Buyer estate which may have fallen outside of mainstream manufacturer / Original Equipment Manufacturer (OEM) support	**Should**
EUS.047	EUS Security	**End User Services**	The Supplier must manage the disposal of the range of hardware that is specified in types of IT equipment for disposal in line with the policies and standards set out in the Buyer's Disposal Policy	**Must**
EUS.048	EUS Services & Support	**End User Services**	The Supplier must be responsible for ensuring the Buyer SACM discovery tooling is installed on all Buyer devices and is populating and updating the Buyer CMDB accurately as setout by the Buyer SACM team.	**Must**
EUS.049	EUS Services & Support	**End User Services**	The Supplier must, proactively monitor and resolve the expiry of Asset and Configuration Items (CI), including licenses, tokens and assist the Buyer and Third-Party Suppliers with keeping the information current. The Supplier must (within the agreed Service Levels) be responsible for: (a) responding to queries and requests concerning the hardware and software asset inventory data or supporting information; (b) ensuring that all deployment of software procured by the Buyer or the Supplier is compliant with the number of purchased licenses; and (c) conducting assurance reviews and audits and provide evidence to the Buyer and its auditors of the accuracy and completeness of the records in the Buyer CMDB and the existence of CIs.	**Must**
EUS.050	EUS Services & Support	**End User Services**	The Supplier should, provide and manage testing for releases before they are transferred to the production environments, including testing of any rollback procedures agreed within Buyer back-out plans. The Supplier should, maintain and manage the pre-production and test environments for Services, as required, in support of releases.	**Should**
EUS.051	Device Management and Control	**End User Services**	The Supplier should implement (or operate the Buyer's solution) a toolset approved by the Buyer for the remote access to and control of End Users Devices, to facilitate incident and support resolution.	**Should**
EUS.052	Catalogue and Request	**End User Services**	The Supplier should in response to a standard Service Catalogue Request, administer ownership changes to SharePoint sites (Including but not limited to additions, removals and changes to owners of the sites).	**Should**
EUS.053	EUS Services & Support	**End User Services**	The Supplier should manage the provisioning and support of user accounts that cannot be automatically provisioned by any of the Buyer HR systems (including but not limited to contractors, Suppliers or other third parties who provide a service to the Buyer).	**Should**
EUS.054	EUS Services & Support	**End User Services**	The Supplier should manage the user accounts that remain in the Buyer defined legacy domains, including group memberships, access to file stores and applications, GPOs, and other user management related tasks	**Should**
EUS.055	PKI Services	**End User Services**	The Supplier must provide, maintain and support certificate enrolment.	**Must**
EUS.056	PKI Services	**End User Services**	The Supplier must provide Public Key Infrastructure to the Buyer and Other Core Defra Group Suppliers to support all certificate related functions including the encryption of data in transit including: (a)VPNs; (b)client; (c)server or network endpoint authentication; (d)network access control; (e)messaging and file encryption; (f)code signing; (g)integrity checking; (h) non-repudiation; and (i) digital signature services.	**Must**
EUS.057	PKI Services	**End User Services**	The Supplier must work with the Other Core Defra Group Suppliers in the provision of certificate and key management services.	**Must**
EUS.058	PKI Services	**End User Services**	The Supplier must provide a registration authority service to process certificate signing requests and certificate revocation requests and will support automated certificate enrolment and issuing for Devices and End Users.	**Must**
EUS.059	PKI Services	**End User Services**	The Supplier must ensure that private keys associated with the Public Key Infrastructure are secured against unauthorised disclosure and modification or loss in line with the Buyer's security policies.	**Must**
EUS.060	PKI Services	**End User Services**	The Supplier must manage certificate revocation for the Public Key Infrastructure service and provide the Buyer and Other Core Defra Group Suppliers with timely notice of certificates that are due to expire.	**Must**

[redacted]

EUS.061	PKI Services	**End User Services**	The Supplier must log and monitor security events and alerts relating to the PKI solution in accordance with the NCSC SOC Data Feeds document. The Supplier must ensure the PKI events are presented for consumption by the Buyer Security Information Event Management System. The Supplier must provide reporting to the Buyer to demonstrate the successful operation of the event and alerting solution, and report to the Buyer on a monthly basis, unless directed otherwise by the Buyer, to demonstrate the successful operation of the PKI solution.	**Must**
EUS.062	PKI Services	**End User Services**	The Supplier must following request by the Buyer, cooperate with and assist the Buyer in relation to the creation and / or update by the Buyer of its Public Key Infrastructure Strategy.	**Must**
EUS.063	EUS Security	**End User Services**	The Supplier must utilise the Buyer's privilege management elevation solution. Where not appropriate ensure that the granting and use of elevated account privileges (including Administrative Privileges) is logged, reviewed and audited at least quarterly. Reports detailing this activity will be provided by the Supplier to the Buyer upon request.	**Must**
EUS.064	IP Addresses	**End User Services**	The Supplier must obtain from the Connectivity Supplier, IP address ranges for the provision of its Services in accordance with the IP Address Management Architecture Design and Guidance.	**Must**
EUS.065	IP Addresses	**End User Services**	The Supplier must for any Services presented to the live environment, only use the IP addresses provided to them by the Connectivity Supplier, unless otherwise agreed with the Buyer.	**Must**
EUS.066	IP Addresses	**End User Services**	The Supplier must manage the allocation of IP addresses provided by the Buyer's Connectivity Supplier to deliver its Services in line with best industry practice.	**Must**
EUS.067	Application Packaging, Virtualisation Deployment & Support	**End User Services**	The Supplier should manage and support an agreed portal where applications that are pre-approved by the Buyer are published or otherwise made available for download by the End User. This will comply with the concept of "default allow" whereby End Users can access and be licensed for applications on a centralised corporate basis	**Should**
EUS.068	Application Packaging, Virtualisation Deployment & Support	**End User Services**	In so far that it can be done under the Tech Services 3 Framework agreement, the Supplier should provide, manage, package and distribute and support COTS Software packages in agreement with the Buyer.	**Should**
EUS.069	Application Packaging, Virtualisation Deployment & Support	**End User Services**	The Supplier should ensure that COTS Software added to the Service Catalogue is included within Application security patch procedures.	**Should**
EUS.070	EUS Services & Support	**End User Services**	The Supplier should provide a service to provision out of the box End User Devices that are not connected to the network and do not have a Buyer build - for limited (no more than 50 devices at any one time or as agreed with the Buyer) and specific use cases.	**Should**
EUS.071	EUS Services & Support	**End User Services**	The Supplier should provide to the Buyer the facility to assign differing levels of access and software eligibility according to the Persona type assigned to the End User.	**Should**
EUS.072	Application Packaging, Virtualisation Deployment & Support	**End User Services**	The Supplier should ensure that current, new and changed application, platform and infrastructure configurations used in the delivery of the Services are backed up in accordance with the Recovery Time Objective (RTO) and Recovery Point Objective (RPO)	**Should**
EUS.073	EUS Services & Support	**End User Services**	The Supplier should provide, manage and maintain Exchange Hybrid services in-support of M365 environments or any Defra environment or application that relies on those Exchange Hybrid services. Supplier should also ensure that the following key elements of the service are supported, managed and maintained; (a)unified Global Address List (GAL); (b)the free/busy and calendar sharing between on-premises and Exchange Online; (c)enable other Buyer applications to relay email data via the Exchange service; (d)the inbound and outbound electronic mail (email) flow; (e)provide centralised mailbox management for both on premise and cloud Exchange to Other Core Defra Group Suppliers; (f)and support a backup and recovery service in support of the delivery of the heritage and hybrid exchange services; (g)protect End Users against email based attacks including, phishing, spam, and malware, while maintaining access to email; (h)manage and maintain an archive service for email where the End User is able to retrieve an email from archive by browsing the End User's archive mailbox in EOL archiving; (i)support an email archive service which can perform archive lifecycle management based on age and retention periods; and (j)support an email archive service which enables e-discovery across the archive data set and allows Buyer delegated End Users to recover archived file data.	**Should**
EUS.074	EUS Services & Support	**End User Services**	The Supplier should configure and manage all existing and any new components that are required for the management of the EUS Solution in accordance with the: (a) Buyer's Service Delivery Lifecycle (SMSI-223-001); (b) Approved Services design and Supplier Solution design; and (c) Buyer Enterprise Architecture principles.	**Must**
EUS.075	EUS Services & Support	**End User Services**	The Supplier must use the Domain Name Service (DNS) provided by the Connectivity Supplier or maintain its own subordinate DNS that inter-operates and interfaces with the Connectivity Supplier's Domain Name Service (DNS).	**Must**
EUS.076	EUS Services & Support	**End User Services**	The Supplier shall ensure all components and Devices used in the delivery of its Services have their time synchronised to a Master Time Reference Service as agreed by the Buyer.	**Must**

[redacted]

EUS.077	EUS Services & Support	**End User Services**	The Supplier must provide rapid response support services (in-line with the timescales setout in the Call Off Schedule 3 (Service Levels, Service Credits and Performance Monitoring)) to the Buyer during times of national emergency situations. Invocation of emergency situations must be initiated by nominated authorised Buyer personnel. The support must include but not be limited to the following services: •Support at any location (including non-Buyer sites) in mainland UK and islands; •On site engineering resource presence to provide technical support in configuring devices, peripherals and identified technology services required for the management of the emergency situation; •Technical support of users associated with the emergency situation; •Emergency site commissioning of IT services, including co-ordination activities across the Buyer and its IT Service providers (i.e. Security / Networks / Managed print etc). Site commissioning and support provision to commence immediately upon emergency invocation; •Fulfil device or hardware requirements within 24 hours notice of emergency situation by the Buyer; •Working in a flexible, proactive and responsive manner to provide solutions appropriate to the need (which may include use of non-standard solutions to support the emergency invoked); and •Prioritise emergency situations above all other requests and work on a fix/fulfil/respond first basis.	**Must**
EUS.078	Catalogue and Request	**End User Services**	The Supplier must ensure that at all times there will be a minimum of the following stock available for immediate deployment in the event of national emergency situations: •Twenty-five (25) standard Smart Phones •Twenty-five (25) standard Smart Tablets •Twenty-five (25) standard Windows Laptops Requests for deployment of emergency stock holdings should be fulfilled and delivered to the location as specified by the Buyer (including non Buyer locations where the emergency is being managed) within 24 hours of request. Requests in excess of the emergency stock holding must be prioritised and expedited for delivery upon written request by the Buyer.	**Must**
EUS.079	EUS Services & Support	**End User Services**	The Supplier should provide support to the Buyer Geomatics team. The Geomatics team provide customised Geomatics services and integrated spatial data products to the Environment Agency. The Supplier shall support the high specification workstations and Devices used in the delivery of the Geomatics solution (hardware and software support) including the file transfer service that enables digital content to be transferred between the sites.	**Should**

BUYER REQUIREMENTS					BIDDER COMPLIANCE RESPONSE	
ID	Operational Area	Service Function	Requirement	MoSCoW	Fully Compliant Partially Compliant Non-Compliant	COMPLIANCE STATEMENT [MAX 100 Words]
WPE.001	EUS Asset Related	Workplace Enterprise	The Supplier must ensure that the Device specification as detailed in the Minimum Device Specification must meet the Buyer's Connectivity and Architecture Standards and that all Devices are compatible with the Buyer's corporate network including working with all third parties in the delivery, support and maintanance including the enablement of access to the Buyers VPN solution on all in scope Devices.	Must	[redacted]	[redacted]
WPE.002	Device Management	Workplace Enterprise	The Supplier must ensure that End Users can access offline data stored on all Devices (including desktops, laptops and Smart Devices), whether it's connected or not connected to the Buyer's ICT Environment.	Must		
WPE.003	Device Management	Workplace Enterprise	The Supplier must make best endeavour to ensure that no data replicated to the cloud is lost or corrupted when repairing, restoring or replacing any Device or any software as part of the services.	Must		
WPE.004	Device Management	Workplace Enterprise	Any service requests by the End User to the Service Desk as a result of the Supplier failing to configure the Device for use correctly must be at the Suppliers cost.	Must		
WPE.005	Device Management	Workplace Enterprise	The Supplier must enable managed and automated deployment of operating system upgrades, cumulative updates, patches and security fixes for all Devices in line with policies defined by the Buyer.	Must		
WPE.006	Device Management	Workplace Enterprise	The Supplier must ensure that the End User is able to perform password resets without the need for Supplier or Service Desk intervention across all Devices.	Must		
WPE.007	Device Management	Workplace Enterprise	The Supplier must be able to remotely reset Smart Device passcodes using the approved device management solution.	Must		
WPE.008	Device Management	Workplace Enterprise	The Supplier must provide mechanisms to facilitate Single Sign-On (SSO) for a defined set of applications and services agreed with the Buyer.	Must		
WPE.009	Device Management	Workplace Enterprise	All Devices must be enrolled and managed by the Buyer's Microsoft Intune (or its replacement) Device Management Infrastructure	Must		
WPE.010	Device Management	Workplace Enterprise	The Supplier must provide, support and maintain Modern Device Management services, including but not limited to: (a) policy settings; (b) restrictions; (c) Wi-Fi profiles; (d) email profiles; (e) Application default allowed list; (f) Device management (inventory); (g) reset/wipe/lock; (h) encrypt Device; (i) set password policy; and (j) configure Device settings (browser and app settings, firewall configuration, remote assistance, Software management).	Must		
WPE.011	Application Packaging, Virtualisation Deployment & Support	Workplace Enterprise	The Supplier must support the existing application packaging technology service and identify continuous improvement opportunities, including but not limited to automation of activities where possible.	Must		
WPE.012	Device Management	Workplace Enterprise	The Supplier must maintain and support the registration of the Buyer Devices through Apple Business Manager for all Apple Devices. This includes ensuring all identified existing Devices are registered in the Apple Business Manager.	Must		
WPE.013	Device Management	Workplace Enterprise	The Supplier must ensure that all in-scope Devices are auto-assigned or auto enrolled securely to the Buyer's Intune platform before assigned to an End User for use.	Must		
WPE.014	Device Management	Workplace Enterprise	The supplier should deliver equivalent functionality and access from a service perspective, in support of corporately owned, privately enabled (COPE) non-Windows operating system Devices including, but not limited to, configurations such as: (a) control settings; (b) existing restrictions, security policies, certificates and access to existing public cloud app stores; (c) Certificates; (d) All existing profiles e.g. email, Wi-Fi, security; (e) browser whitelisting (like-for-like); (f) Managed Application Stores; (g) Device management (inventory); (h) reset/wipe/lock; (i) encrypt Device; (j) set password/passcode policies; (k) configure Device settings (browser and app settings, firewall configuration, remote assistance, Software management); and (l) Current Managed Applications and VPN Profiles available and working to users.	Should		
WPE.015	Device Management	Workplace Enterprise	The Supplier must work with the Buyer's third party supplier eco-system, including the existing systems and processes to ensure Devices are successfully enrolled into the Buyer's management platforms	Must		
WPE.016	EUS Asset Related	Workplace Enterprise	1. The Supplier should provide Devices to End Users in line with Service Levels. 2. The Supplier should ensure all Devices are asset tagged and Device details are recorded in accordance with the Buyer's Hardware Asset Management Policy before deployment to the End User.	Should		
WPE.017	Device Management	Workplace Enterprise	The Supplier should have the ability to disable or remotely wipe, disable, reset or manage any Device through Microsoft Intune(or its replacement), or Device management capability supported by the Device, upon instruction from the Buyer or inline with any runbook or operational management instruction.	Should		

WPE.018	EUS Asset Related	**Workplace Enterprise**	The Supplier must repair, refurbish, reset, re-configure and re-issue Buyer Devices to End Users as part of the Lifecycle Management of Devices process.	**Must**
WPE.019	EUS Services & Support	**Workplace Enterprise**	The Supplier must manage and support the use of shared Devices, including but not limited to iPads,kiosks and Desktops that are used by internal and external staff.	**Must**
WPE.020	Device Management	**Workplace Enterprise**	The Supplier must be registered, or to ensure its third party hardware suppliers to be registered with Android Enterprise, for the provision of new Android Devices for the Buyer.	**Must**
WPE.021	EUS Security	**Workplace Enterprise**	The Supplier must ensure that the Device security posture is maintained in line with the Buyer's security policies.	**Must**
WPE.022	Application Packagir	**Workplace Enterprise**	The Supplier must maintain and support operating system update deployment rings in the Buyer environment.	**Must**
WPE.023	Device Management	**Workplace Enterprise**	The Supplier must manage major updates to operating systems, such as the migration from Windows 10 to Windows 11 or later version releases using modern managed deployment practices.	**Must**
WPE.024	Device Management	**Workplace Enterprise**	The Supplier should support the Autopatch features and functionality in the Microsoft 365 enterprise-level version suite.	**Should**
WPE.025	EUS Services & Support	**Workplace Enterprise**	The Supplier should ensure the Buyer End User application community is engaged, actively involved in application testing that occurs as part of any OS upgrade implementation	**Should**
WPE.026	EUS Security	**Workplace Enterprise**	The Supplier must manage and support secure user access to the Buyer's applications and services in Microsoft 365 across different platforms (applications/browsers) and Devices as set-out with within the Buyer's security policies.	**Must**
WPE.027	EUS Services & Sup	**Workplace Enterprise**	1. The Supplier should provide and deliver a consistent remote support tooling experience to End Users that is operating system agnostic (supporting Android, Windows, iOS and MacOS operating systems) 2. The Remote Management software tooling must integrate with Microsoft Intune and ServiceNow. 3. The Supplier should not utilise different remote management toolsets for different aspects of the service if possible.	**Should**
WPE.028	Digital Workplace	**Workplace Enterprise**	The Supplier must operate the service in compliance with the Defra group ICT Technical Vulnerability Management Policy.	**Must**
WPE.029	Digital Workplace	**Workplace Enterprise**	The Supplier must have the capability, mechanisms and processes to review and analyse the security posture of the Buyer's IT estate on an ongoing basis and report findings and deviations from the Buyer security standards.	**Must**
WPE.030	Digital Workplace	**Workplace Enterprise**	The Supplier must provide (on an ongoing basis) visibility into the Buyer's applications and software inventory (i.e. versions, patch level etc), both deployed and in use across the enterprise, including web-based applications (where possible).	**Must**
WPE.031	Digital Workplace	**Workplace Enterprise**	The Supplier must generate Vulnerability Management reports and dashboards in the format and frequency stipulated in the Defra group ICT Technical Vulnerability Management Policy.	**Must**
WPE.032	Digital Workplace	**Workplace Enterprise**	The Supplier must, when a critical vulnerability is identified provide the Buyer with detailed information relating to the Vulnerability identified and manage the resolution through the Incident Management process.	**Must**
WPE.033	Digital Workplace	**Workplace Enterprise**	The Supplier must remediate critical vulnerabilities within the time frames identified within the Defra group ICT Technical Vulnerability Management Policy.	**Must**
WPE.034	Digital Workplace	**Workplace Enterprise**	The Supplier must accept and respond to incident tickets that the Buyer's Security Operations Centre (SOC) may raise as a result of the threat alerts.	**Must**
WPE.035	Digital Workplace	**Workplace Enterprise**	The Supplier must have processes in place to remain aware of all new and existing vulnerabilities published in relation to the hardware, firmware and software associated with all End User Devices.	**Must**
WPE.036	Digital Workplace	**Workplace Enterprise**	The Supplier must carry out risk assessments of all vulnerabilities within the Suppliers scope of services and apply remediation in accordance with the criteria, timescales and processes as set out in the Defra group ICT Technical Vulnerability Management Policy or as agreed with the Buyer.	**Must**
WPE.037	EUS Security	**Workplace Enterprise**	The Supplier must operate the Buyer's Data Loss Protection solution including the deployment of Data Loss Protection policies that have been agreed with the Buyer, that can monitor, capture and prevent the movement / copying of file meta data between file systems and removable media	**Must**
WPE.038	EUS Security	**Workplace Enterprise**	The Supplier must secure data 'in transit' against tampering, loss and eavesdropping as set out in the Defra Group Data Loss Prevention Policy.	**Must**
WPE.039	EUS Security	**Workplace Enterprise**	The Supplier must secure data at rest through security controls that meet the standards set out in the Data Loss Protection policies	**Must**
WPE.040	EUS Security	**Workplace Enterprise**	The Supplier must use Data Loss Protection controls to classify and prioritise information security in order to manage and monitor unauthorised data egress.	**Must**
WPE.041	EUS Security	**Workplace Enterprise**	The Supplier should provide USB device control solutions that provides as a minimum: Allow users to connect standard HID (Human Interface Devices) based USB equipment for Input/output. HID allowed devices should not control USB Ports Recording of USB Devices that are inserted or removed from Buyer managed devices. The scanning of mass storage Devices for Malware and virus' to support AV and DLP controls.	**Should**
WPE.042	EUS Security	**Workplace Enterprise**	The Supplier should offer endpoint access management, allowing specified users (administrators) to control access to Buyer End User Devices and enforce policies based on user roles and security levels.	**Should**
WPE.043	Application Packaging, Virtualisation Deployment & Support	**Workplace Enterprise**	The Supplier must manage, maintain, support and operate the Buyer's application virtualisation and presentation service. The service responsibilities include but are not limited to: •Operational support of the Buyer Citrix, VMWare Horizon, Windows 365 and Azure Virtualisation Desktop Environments •Support of Applications and Services delivered by the virtualisation and presentation service •Support the Buyer in the migration of Applications and Services between the virtualisation technologies •Onboarding of new and/or replacement Applications onto the virtualisation services •Decommissioning and removal of Applications and Services from the environments as requested	**Must**

[redacted]

WPE.044	Application Packaging, Virtualisation Deployment & Support	**Workplace Enterprise**	The Supplier must manage, maintain, support and operate an application packaging and deployment service utilising the Buyer tooling. The service responsibilities include but are not limited to: •Upgrade of application versions in the Buyer estate •Automated deployment of updated applications to End User Devices •Management of application versions and reporting to the Buyer end of life / end of support versions within the environment •Packaging and deployment of new applications in to the estate upon request by the Buyer •Decommissioning and removal of applications from the estate upon request by the Buyer •Support and maintenance of the presentation and deployment service and all of its infrastructure components •Integration with Buyer defined tools and services	**Must**	

[redacted]

BUYER REQUIREMENTS					BIDDER COMPLIANCE RESPONSE	
ID	Operational Area	Service Function	Requirement	MoSCoW	Fully Compliant Partially Compliant	COMPLIANCE STATEMENT [MAX 100 Words]
VCS.001	Enterprise Collaboration	**Video Conferencing & Microsoft Teams Room Support**	The Supplier shall provide proactive monitoring of the in scope VC Hardware during core operational hours (07:00-19:00). Issues identified as a result of Pro-active monitoring should follow the Buyer Incident management process, resolving incidents remotely wherever possible.	**Must**	[redacted]	[redacted]
VCS.002	Enterprise Collaboration	**Video Conferencing & Microsoft Teams Room Support**	The Supplier shall ensure that the agreed end point performance and analytical tool is operating on all in-scope VC Hardware and that this information is reporting in to centralised monitoring dashboards. The Buyer shall have access to all dashboards views.	**Must**		
VCS.003	Enterprise Collaboration	**Video Conferencing & Microsoft Teams Room Support**	The Supplier shall ensure that all networked VC Hardware is capable of being remotely managed, controlled and repaired. The Supplier shall ensure that remote managed, controlled and repaired tasks shall be performed successfully in line with the best industry standards.	**Must**		
VCS.004	Enterprise Collaboration	**Video Conferencing & Microsoft Teams Room Support**	The Supplier shall ensure that the in Scope VC Hardware receives maintenance, security and firmware updates in accordance with appropriate manufacturer guidelnes and deployed in a schedule agreed with the Buyer in advance	**Must**		
VCS.005	Enterprise Collaboration	**Video Conferencing & Microsoft Teams Room Support**	The Supplier shall upon request from the Buyer procure (on behalf of the Buyer), ship, install and configire any new or replacement VC Hardware equipment in accordance with the Buyer's VC Hardware Minimum Specification. Installation and configuration includes ensuring VC Hardware is correctly connected to the Buyer's network and is enrolled for performance and device management and that the AV set up is suitable and functioning when connecting up to an in-room AV solution when provisioning and installing VC Hardware.	**Must**		
VCS.006	Enterprise Collaboration	**Video Conferencing & Microsoft Teams Room Support**	The Supplier shall upon request from the Buyer increase or decrease the volume of VC Hardware installations. All installations activities (additions or removals) shall be in accordance with the Buyer VC installation standards.	**Should**		
VCS.007	Enterprise Collaboration	**Video Conferencing & Microsoft Teams Room Support**	The Supplier shall where the Buyer site has a Tech Bar, provide onsite technical support to the in scope VC Hardware to the extent possible without recourse to specialist hardware or software installation, support could include but not limited to reseating of VC connections (e.g. network, power, video, audio), configuration of Microsoft Teams, help advice and guidance to end users.	**Must**		
VCS.008	Enterprise Collaboration	**Video Conferencing & Microsoft Teams Room Support**	The Supplier shall work with the Buyer to provision flexible short term loans of mobile VC solutions (such as JabraPanacast cameras and associated peripherals) - this could be via Vending solutions, Smart Lockers or Tech Bars provisions. All solutions will be agreed with the Buyer in advance of implementation	**Should**		
VCS.009	Enterprise Collaboration	**Video Conferencing & Microsoft Teams Room Support**	The Supplier should work collaboratively with Defra's Connectivity supplier in the support and management of Defra's meeting room panels ensuring that issues are identified and assigned to the supplier who is responsible for the item or service with an issue.	**Should**		
VCS.010	Enterprise Collaboration	**Video Conferencing & Microsoft Teams Room Support**	The Supplier shall inform the Buyer if any AV equipment is not compatible or should become incompatible due to system updates or similar either in a new or exisiting installation.	**Should**		

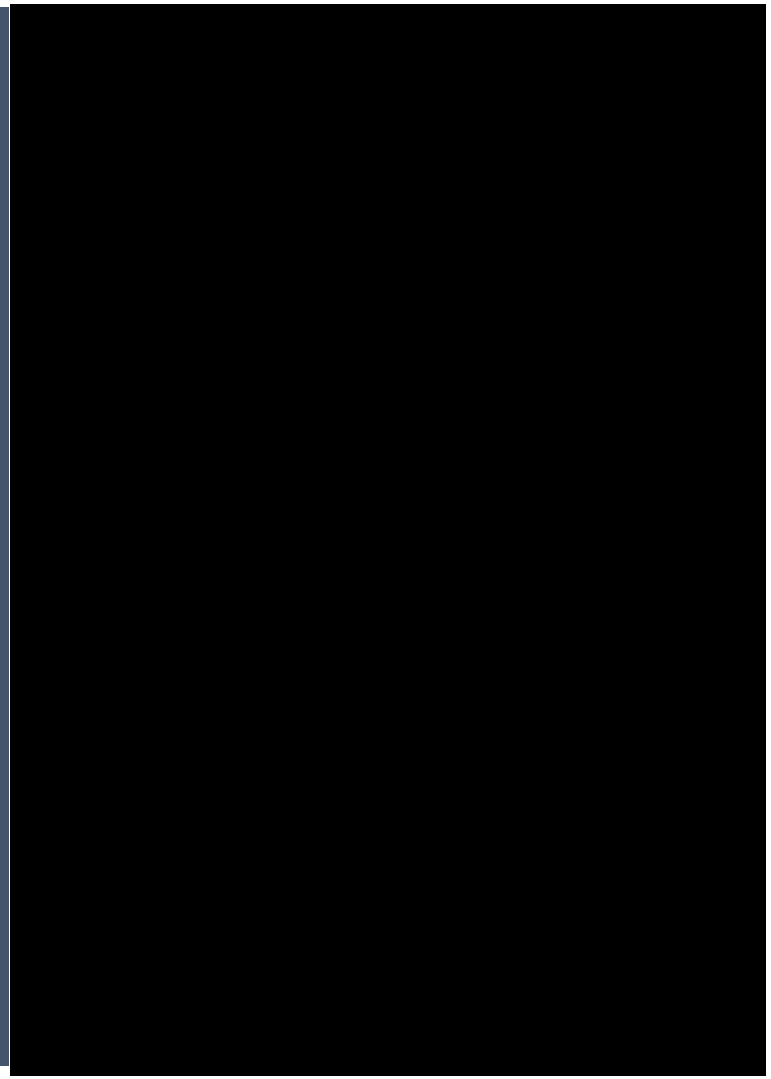
BUYER REQUIREMENTS					BIDDER COMPLIANCE RESPONSE	
ID	Operational Area	Service Function	Requirement	MoSCoW	Fully Compliant Partially Compliant Non-Compliant	COMPLIANCE STATEMENT [MAX 100 Words]
DEX.001	Digital Experience Performance Monitoring	Digital User Experience	The Supplier must ensure that there is performance and experience monitoring in place for Device hardware, operating system, network performance and software applications running on the Device. The monitoring output should be captured in a repository that can be reported on via a console / dashboard accessible by the Supplier or authorised Buyer teams. The Supplier shall propose remediation options, including a documented policy and process for Device refresh to be approved by the Buyer and enacted by the Supplier once approved, for any Device falling below the agreed baseline performance levels to the Buyer and shall ensure that the Buyers ITSM Tool (ServiceNow) will be utilised to support remediation activities (for example, automatically triggering the issuance of knowledge based articles or arrange a repair or provisioning a replacement Device).	Must		[redacted]
DEX.002	Digital Experience Performance Monitoring	Digital User Experience	The Supplier must manage the end user device asset refresh according to the Buyer's preferred Device refresh cycle. Devices will only be replaced where they cannot be refurbished or repaired. The Supplier will replace the device with re-used equipment (refurbished, remanufactured) in the first instance and only replace with new devices as per the Device performance analytics based on user experience, behaviours and device health check where there is performance degradation identified in a device that cannot be remediated.	Must		
DEX.003	Digital Experience Performance Monitoring	Digital User Experience	The Supplier must maintain all End User Devices for its Services, and any relevant parts, measured against the current industry standard (as at the date of such maintenance), taking into account the nature of the Services for the relevant Device, asset or part, as appropriate, so that any new or replacement Devices, assets or parts, as appropriate, shall: (i) have an equivalent or greater anticipated lifespan; (ii) avoid technological obsolescence or failure; and, (iii) be of sufficient quality to deliver the Services in accordance with the Buyer's request	Must		
DEX.004	Digital Experience Performance Monitoring	Digital User Experience	The Supplier must deploy Digital Experience (DEX) Service for the Buyer. The Supplier will integrate the DEX service into the Buyer's ITSM Tool (ServiceNow).	Must		
DEX.005	Digital Experience Performance Monitoring	Digital User Experience	Th Supplier should produce a Digital User Experience Architecture High Level Design, consulting with the Buyer and it's other Core Defra Group Suppliers as appropriate. The design should undergo the Buyer's 'Technical Design Authority (TDA)' Governance sign off prior to any implementation.	Must		
DEX.006	Digital Experience Performance Monitoring	Digital User Experience	The Supplier will deploy the DEX client to the Buyer end user devices. The Buyer's analytics information from the End User Devices will be fully available in the DEX tool Instance. Additionally certain information will also be available within the Buyer's ITSM Tool (ServiceNow) as agreed with the Buyer.	Must		
DEX.007	Digital Experience Performance Monitoring	Digital User Experience	Maintain and update the Digital User Experience Architecture High Level Design in line with project infrastructure change and provide an updated version at the request of the Buyer up to a maximum of three (3) times per year.	Must		
DEX.008	Digital Experience Performance Monitoring	Digital User Experience	Produce a Digital User Experience Architecture Low Level Design, consulting with the Buyer and it's other Core Suppliers as appropriate. The design is not subject to the Buyer's 'Technical Design Buyer' Governance but should be made available to the Buyer on request.	Should		
DEX.009	Digital Experience Performance Monitoring	Digital User Experience	The Digital User Experience service must have the capability of measuring external SaaS services including MS Teams / O365 and well as internal Defra group Application accessed via the RAS solution.	Must		
DEX.010	Digital Experience Performance Monitoring	Digital User Experience	The Digital User Experience service should be capable of monitoring a minimum of 25 external and 25 internal applications, whilst also allowing dynamic re-configuration of monitored endpoints as required.	Should		
DEX.011	Digital Experience Performance Monitoring	Digital User Experience	The Digital User Experience service must be capable of monitoring and identifying the following: (a) Bottlenecks in the end to end service that impacts the User experience (b) Component level performance that contribute to the Devices falling below the agreed performance metric to instigate refresh or repair.	Must		
DEX.012	Digital Experience Performance Monitoring	Digital User Experience	The Supplier must ensure the Digital User Experience monitoring portal / dashboard (via a standard browser) is made available to Buyer and Core Defra Group Supplier users to view reporting, support troubleshooting or incident resolution. The portal shall meet the service requirements outlined under Service Manangement. Where additional access is required, the Supplier shall highlight what is required and work with the Buyer to deliver configuration.	Must		
DEX.013	Digital Experience Performance Monitoring	Digital User Experience	The portal should use an intuitive GUI to enable the customer to view information by individual user, site location, agency or service performance	Should		
DEX.014	Digital Experience Performance Monitoring	Digital User Experience	The service should display performance in a format that is straightforward to interpret good, variable and poor performance, along with root cause, at a high level	Should		
DEX.015	Digital Experience Performance Monitoring	Digital User Experience	The service should load any data or searches in reasonable timeframe for any investigations, interrogations or reports	Should		
DEX.016	Digital Experience Performance Monitoring	Digital User Experience	The service should ensure that the digital experience per CI is monitored end to end, as needed for end user, site location, agency and service	Should		
DEX.017	Digital Experience Performance Monitoring	Digital User Experience	The Buyer can view individual user, group of defined users, individual service, group of defined services, agency and individual site performance within the service	Should		
DEX.018	Digital Experience Performance Monitoring	Digital User Experience	The service can compare performance between service baseline and changes to baseline, and between different Devices	Should		
DEX.019	Digital Experience Performance Monitoring	Digital User Experience	The portal should have a minimum of 12 months data available to interrogate	Should		
DEX.020	Digital Experience Performance Monitoring	Digital User Experience	The service must show all end to end performance response times and identified CI's in routing	Must		
DEX.021	Digital Experience Performance Monitoring	Digital User Experience	The service must take measurements at a suitable frequency to deliver usable information	Must		

DEX.022	Digital Experience Performance Monitoring	**Digital User Experience**	The service must have no noticeable impact to the monitored devices as a result of the service being enabled	**Must**
DEX.023	Digital Experience Performance Monitoring	**Digital User Experience**	The service should be easy to install / update without additional extra cost	**Should**
DEX.024	Digital Experience Performance Monitoring	**Digital User Experience**	The Supplier should ensure that setting up new targets is straightforward / minimal cost & effort.	**Should**
DEX.025	Digital Experience Performance Monitoring	**Digital User Experience**	The number of application targets shall not impact on run costs.	**Should**
DEX.026	Digital Experience Performance Monitoring	**Digital User Experience**	The weighting of targets towards overall individual end user experience should be transparent and adjustable	**Should**
DEX.027	Digital Experience Performance Monitoring	**Digital User Experience**	The Service must proactively identify changes in performance and highlight these back to point in time	**Must**
DEX.028	Digital Experience Performance Monitoring	**Digital User Experience**	The Service should identify changes in performance from established baseline within (24) hours	**Should**
DEX.029	Digital Experience Performance Monitoring	**Digital User Experience**	The Supplier must provide monthly high level reporting summaries on performance to the Buyer to highlight areas of interest or remediation required by end user, site location, agency and service	**Must**
DEX.030	Digital Experience Performance Monitoring	**Digital User Experience**	The report must prioritise issues by impact for end user, site location, agency and service	**Must**
DEX.031	Digital Experience Performance Monitoring	**Digital User Experience**	The Service should be able to translate performance issues into a time/monetary impact to the Buyer, if given appropriate input parameters	**Should**
DEX.032	Digital Experience Performance Monitoring	**Digital User Experience**	The Digital Experience Solution should have the capability for Buyer identified Administrators to create custom reports or dashboards from the captured performance data	**Should**
DEX.033	Digital Experience Performance Monitoring	**Digital User Experience**	The Service data should be exportable in a format agreed with the Buyer.	**Should**
DEX.034	Digital Experience Performance Monitoring	**Digital User Experience**	The Supplier should provide comparisons of the Buyer's End User experience metrics against industry recognised averages. Comparison content and frequencey will be in agreement with the Buyer.	**Should**
DEX.035	Digital Experience Performance Monitoring	**Digital User Experience**	The Supplier should provide the Buyer with access to training material, collateral and in person training sessions as agreed between the parties.	**Should**
DEX.036	Digital Experience Performance Monitoring	**Digital User Experience**	The Supplier shall be responsible for supplying, monitoring and managing the DEX solution roadmap for enhancements upgrades and additional features which will be fully available to the Buyer as part of regular reporting and governance. The effectiveness of this monitoring and management activity shall be evidenced through the Supplier use of DEX solution is an integral part of Continual Service Improvement and enhancement initiatives delivering measurable value to the Buyer.	**Should**
DEX.037	Digital Experience Performance Monitoring	**Digital User Experience**	The Supplier must provide analytics and information from the Digital Experience tooling to Buyer resolver teams, including third party suppliers to assist with fault finding, incident resolution and root cause analysis where responsibility for the incident resolution falls outside of the Supplier responsibilities.	**Must**

[redacted]

BUYER REQUIREMENTS					BIDDER COMPLIANCE RESPONSE	
ID	Operational Area	Service Function	Requirement	MoSCoW	Fully Compliant Partially Compliant Non-Compliant	COMPLIANCE STATEMENT [MAX 100 Words]
ATS.001	Digital Workplace	**Assistive Technology Services**	The Supplier must ensure that all of the Assistive Technology Services adhere to the Buyer's approved Assistive Technology policies.	**Must**	[redacted]	[redacted]
ATS.002	Digital Workplace	**Assistive Technology Services**	The Supplier must support the Assistive Technology End Users' needs in any Buyer Premises, and where required, for UK home-based workers.	**Must**		
ATS.003	Digital Workplace	**Assistive Technology Services**	The Supplier must provide, support and manage existing range of Assistive Technology products that are used by Assistive Technology users, that must include but not be limited to the products detailed in Assistive Technology Product List.	**Must**		
ATS.004	Digital Workplace	**Assistive Technology Services**	The Supplier must provide, manage and maintain Assistive Technology tools that enable staff with disabilities (including but not limited to neurodiversity).	**Must**		
ATS.005	Digital Workplace	**Assistive Technology Services**	The Supplier should work with the Buyer to create an initial Assistive Technology road map within 3 months of initial contract. The Supplier should update and maintain in conjunction with the Buyer at least every 6 months, providing insight and technology change information.	**Should**		
ATS.006	Digital Workplace	**Assistive Technology Services**	The Supplier must maintain a consistent view of the new and emerging technology capabilities available with regards to Assistive Technology. The Supplier will provide on a regular basis updates to the Buyer (at least quarterly) on relevant changes in the Assistive technology market which the Buyer may benefit from.	**Must**		
ATS.007	Digital Workplace	**Assistive Technology Services**	The Supplier must work with the Buyer to gain knowledge of the Buyer's Assistive Technology User community demographics and proactively recommend tools and products that better meet user needs. The information needs to be held securely and accessed only by appropriate Supplier personnel (for sensitivity and data protection purposes).	**Must**		
ATS.008	Digital Workplace	**Assistive Technology Services**	The Supplier must ensure all software upgrades are reflected through the Buyer's chosen tooling (currently this is ServiceNow) and conducted in accordance with the Buyer's Service Management Process.	**Must**		
ATS.009	Digital Workplace	**Assistive Technology Services**	The Supplier should ensure that Assistive Technology software [as detailed in the Assistive Technology Product List] is maintained at the most recent stable release version as advertised by the software Manufacturer. Maintained means that software is tested for compatibility with the Buyer devices and operating systems and is packaged for deployment and made available for authorised users to download, install and use. The Supplier should proactively carry out this activity without need for the Buyer to request.	**Should**		
ATS.010	Digital Workplace	**Assistive Technology Services**	The Supplier should advise the Buyer when updates of Assistive Technology software [as detailed in the Assistive Technology Product List] is available for deployment to users. The Supplier should provide technical assistance to the Buyer AT team for the purposes of User Acceptance Testing (UAT) to ensure the software is working as required by users and any features that need training or additional support can be produced. The Supplier should deploy updated software to designated UAT devices as defined by the Buyer AT team.	**Should**		
ATS.011	Digital Workplace	**Assistive Technology Services**	The Supplier must identify Assistive Technology Users who have been identified to have recommended reasonable IT based adjustments under the Equality Act 2010 from Department of Work and Pensions Access to Work Grant, Display Screen Equipment (DSE), Occupational Health or Workplace Assessments. The Supplier must provide monthly reports of Assistive Technology identified users and their Assistive Technology provided solutions. The Supplier must provide ad-hoc reports of the Buyer Assistive Technology user base upon request by the Buyer within 48 hours of receiving the request. The Supplier must use the Buyers ITSM tooling to for data capture and reporting purposes wherever possible. Data relating to the Assistive Technology Service held in any other system needs to be approved by the Buyer in advance.	**Must**		
ATS.012	Digital Workplace	**Assistive Technology Services**	The Supplier must ensure that their personnel providing support to Assistive Technology Users are subject matter experts with knowledge, skills and competency in Assistive Technologies and prior experience in working with Assistive Technology Users.	**Must**		
ATS.013	Digital Workplace	**Assistive Technology Services**	The Supplier must provide an Assistive Technology Lead who will be accountable for the Suppliers Assistive Technology service and a point of contact at Supplier for the Authority to engage with.	**Must**		
ATS.014	Digital Workplace	**Assistive Technology Services**	The Supplier should fulfil Assistive Technology Non Standard Service Requests and adhere to the Buyer NSSR process and Service Catalogue Management process and policy.	**Should**		

ATS.015	Digital Workplace	**Assistive Technology Services**	The Supplier must provide in person support in the Buyer Defined Locations for End Users, including Assistive Technology Users.	**Should**
ATS.016	Digital Workplace	**Assistive Technology Services**	The Supplier should provide on demand, End User Home visit support calls to users with Assistive Technology needs. This will be a call off chargeable service in line with agreed contractual rates. The Supplier should ensure that any End User home support provision is carried out by staff with Assistive Technology experience, necessary security clearance and has appropriate insurance cover as set out by the Buyer.	**Should**
ATS.017	Digital Workplace	**Assistive Technology Services**	The Supplier must ensure all Supplier resources and delivery staff are fully insured to carry, deliver and install equipment and software to Assistive Technology User's home address. Supplier to ensure their 3rd Party couriers are fully insured to carry and deliver equipment and software to Assistive Technology User's home addresses.	**Must**
ATS.018	Digital Workplace	**Assistive Technology Services**	1. The Supplier must enable the provision of home visits for Assistive Technology support with a specialist service approach, characterised by attention to detail, convenience, speed, and emotional and sensitive considerations of the End User. 2. The Supplier must demonstrate conformity to the Buyer Code of Conduct and uphold the desired behaviours when interacting with Assistive Technology users. Supplier to ensure home visit engineers are EDI trained. 3. Supplier to ensure home visit engineers are briefed beforehand by Supplier's Assistive Technology Service. 4. Supplier to ensure their central Assistive Technology Service are contactable by home visit engineer in case of queries during home visit.	**Must**
ATS.019	Digital Workplace	**Assistive Technology Services**	The Supplier should provide User Guides in a format appropriate for the user of the Assistive Technology (e.g. audio for visually impaired) to enable the End User to become familiar with the Assitive Technology provided for their needs. The Supplier should in conjunction with the Buyer review and update as needed the User Guides and associated Assistive Technology Knowledge Articles on an annual basis or within 1 month of any Assistive Technology changes into production.	**Should**
ATS.020	Digital Workplace	**Assistive Technology Services**	The Supplier should provide training to End Users in the effective use of Buyer provided hardware and software for Users identified as having Assistive Technology needs.	**Should**
ATS.021	Digital Workplace	**Assistive Technology Services**	The Supplier should ensure that specialist Assistive Technology vendors are utilised as part of hardware and software provision to the Buyer. The Supplier should detail which specialist Suppliers they use and highlight the specialists credentials within Assistive Technology provision. The Supplier should provide to the Buyer demonstrations of Assistive Technology hardware and software on a regular basis (no less than once per annum) The Supplier should provide to the Buyer training in the use of Assistive Technology hardware and Software	**Should**
ATS.022	Digital Workplace	**Assistive Technology Services**	The Supplier must ensure that all staff providing services or support to Assistive Technology User's have completed mandatory training in: Equality, Diversity and Inclusivity, which is renewed on an annual basis. Evidence of completed training must be provided to the Buyer annually.	**Must**
ATS.023	Digital Workplace	**Assistive Technology Services**	The Supplier must ensure that all Assitive Technology Incidents and Service Requests are managed in line with the Buyers Incident Management and Request Fulfilment Policies. The Buyer retains the right at its sole discretion to escalate and increase the priority of Incidents or the Service Requests as it deems necessary.	**Must**
ATS.024	Digital Workplace	**Assistive Technology Services**	The Supplier should provide monthly reports on the usage of Assistive Technology Software across the Buyer user base. The Supplier should provide ad-Hoc reports of AT software usage across the Buyer user base upon request by the Buyer within 48 hours of receiving the request.	**Should**
ATS.025	Digital Workplace	**Assistive Technology Services**	The Supplier should as part of monthly reporting and governance propose to the Buyer opportunities and initiatives to improve the Assistive Technology service to end users. Continuous Improvement initiatives (where approved by the Buyer for implementation) are to be monitored and tracked for effectiveness.	**Should**
ATS.026	Digital Workplace	**Assistive Technology Services**	The Supplier must assign a minimum Priority rating of three to all incidents received that involve End User Assistive Technology software issues.	**Must**



BUYER REQUIREMENTS					BIDDER COMPLIANCE RESPONSE	
ID	Operational Area	Service Function	Requirement	MoSCoW	Fully Compliant Partially Compliant Non-Compliant	COMPLIANCE STATEMENT [MAX 100 Words]
MPS.001	Microsoft 365 Product & Platform	**Microsoft 365 Product & Platform Support**	The Supplier must provide operational support to the M365, Intune and associated Microsoft products and services in use by the Buyer's End Users. The Supplier must perform all activities that can be completed as a result of being assigned delegated permissions by the Buyer that are aligned to the role based standards, assigned by Microsoft and set out in the the Azure Active Directory Role Delegation document. For the avoidance of doubt, support activities are classed as: A repeatable task, action or support (advice) requested by a Buyer's User that a supplier can complete on behalf of the Buyer within the roles and permissions granted using the Microsoft 365, Intune and associated products and in accordance with their core functionality and aligned to Microsoft usage guidance. M365 and InTune Products and Services in use will be reviewed and agreed between the parties on a regular basis and no less than every 6 months.	**Must**	[redacted]	
MPS.002	Microsoft 365 Product & Platform	**Microsoft 365 Product & Platform Support**	The Supplier should ensure support procedures are carried out in accordance with and aligned to Defra's security and architectural policies at all times.	**Should**		
MPS.003	Microsoft 365 Product & Platform	**Microsoft 365 Product & Platform Support**	The Supplier will be the primary resolver for all activities that fall within the remit of the delegated Microsoft role permissions (as set out in [AAD Role Delegation for Supplier]. Escalation of issues should only occur if the Suppliers access or role permissions prevent resolution.	**Should**		

BUYER REQUIREMENTS					BIDDER COMPLIANCE RESPONSE	
ID	Operational Area	Service Function	Requirement	MoSCoW	Fully Compliant Partially Compliant Non-Compliant	COMPLIANCE STATEMENT [MAX 100 Words]
BWC.001	Digital Workplace	**Digital Workplace Service & Supplier Management**	The Supplier shall provide a Body Worn Video Service that will administer and support the capture and management of digital video footage, tailored to the Buyer's requirements. This includes the following: a) A private instance of a cloud-based (SaaS) application for the Buyer and its end users to review, annotate, select, redact and share footage; b) Body Worn Cameras are supplied with a USB lead, lanyard and pocket clip (optional accessories are available via the Service Catalogue); c) A software utility to upload footage from the cameras to the cloud application; d) Application administration, performed by remote teams of the Supplier; and e) End User support, consisting of remote teams of the Supplier that will provide specialised application, cameras and support needed for this Service.	**Must**		
BWC.002	Digital Workplace	**Digital Workplace Service & Supplier Management**	The Supplier shall ensure that a) The Body Worn Video Service SaaS application will be accessible to the End Users via an approved internet browser. b) The End Users will be authenticated by reference to the Buyer Azure Active Directory (or its replacement). c) The End Users' account will determine the level of access that the user is granted based on group membership. d) The default retention period for all footage is thirty-one (31) days and the Supplier shall ensure that the footage is deleted by the Supplier or its sub-contractor after this date. e) In the event, that the Buyer requires retention of the footage, the End User will tag the relevant footage within thirty-one (31) days of its creation, where upon the Supplier will ensure that it's Sub-contractor shall retain the footage (including other manipulated copies) for seven (7) years and shall then be deleted by the Supplier or its sub-contractor. f) Any manipulation of the footage causes a separate copy to be created. The application will maintain an audit log of access to, and/or other manipulation of, footage which the Supplier shall ensure will be retained for a period of seven (7) years and shall then be deleted by the Supplier' sub-contractor	**Must**		
BWC.003	Digital Workplace	**Digital Workplace Service & Supplier Management**	The Supplier will provide: a) A software utility that manages the transfer of video footage from the Body Worn Cameras to the SaaS cloud application. b) The camera can be connected by USB cable to a Device, or via a docking station connected to the Uploader PC.	**Must**		
BWC.004	Digital Workplace	**Digital Workplace Service & Supplier Management**	The Supplier shall ensure: a) that the creation of the Buyer's private instance of the cloud application, will be performed by the Supplier or its sub-contractor. b) The application allows users to be assigned into collections, to further control access. For clarity, a collection is the term used for the grouping of users to securely control access to the footage and configure their use of the service. A new collection will be required for a set of new users within the Buyer or a new team of users within an agency that will utilise this Service. c) There is an ability to customise the camera's settings centrally, and any such customisations can be applied to groups of cameras, subject to approval by the Buyer.	**Must**		
BWC.005	Digital Workplace	**Digital Workplace Service & Supplier Management**	The Supplier will integrate the Body Worn Video Service into the Buyer's service management processes.	**Must**		
BWC.006	Digital Workplace	**Digital Workplace Service & Supplier Management**	In the event the Supplier implements a replacement solution over the term, the Supplier shall ensure that: 1. The existing hardware will remain compatible with the replacement solution (or be replaced at the Suppliers cost) 2. The Buyer can maintain file format compatibility with the existing solution in order to access historical files 3. Any existing video footage that is being retained for archival purposes keeps its original date stamp (used for archival / deletion purposes) and can be accessed by any replacement solution. 3. Be wholly responsible for ensuring all relevant files, software and hardware interoperability issues related to transitioning to a replacement solution would be the Suppliers responsibility, with minimal impact to the Buyer.	**Must**		
BWC.007	Digital Workplace	**Digital Workplace Service & Supplier Management**	The Buyer has an exisiting contract for Body Worn Video Service. The Buyer intends to novate this the the Supplier and for the initial period the Body Worn Video shall be delivered by the Supplier through the exisitng supplier.	**Must**		

BUYER REQUIREMENTS					BIDDER COMPLIANCE RESPONSE	
ID	Operational Area	Service Function	Requirement	MoSCoW	Fully Compliant Partially Compliant Non-Compliant	COMPLIANCE STATEMENT [MAX 100 Words]
MBS.001	**Digital Workplace**	**Mobile Service**	The Supplier shall (acting as an authorised agent of the Buyer) perform the following administrative activities in relation to the mobile phone service provided by the Buyer's Mobile Services Provider, by utilising the Mobile Services Providers corporate service administration portal and online tooling to complete the following types of activities that include but are not limited to: a) Provision a connection b) Cease a connection c) Create monthly itemised invoice reporting by user/organisation within the Core Defra Group d) Enable self-service users to identify and label user subscriptions with a username and cost centre (when required) to enable the reporting functionality via the Self-Service Portal, including but not limited to the Billing Management Application (BMA). e) Provide all billing data fully itemised in its most granular form. f) Enable notifications (by email) to account administrators of the availability of their invoice/s and any associated billing information which is made available via the Billing Management Application (BMA) of the Self-Service Portal. g) Liaise with the Buyer's Mobile Services provider via communications channels (such as online 'chat') to provide support to the Buyers Users in 'real-time' h) Perform approved actions against a registered SIM or connection (i.e. call plan changes, activation of features and functions) i) Action the Buyer requests for service fulfilment j) Generate reports on mobile usage to allow the Buyer to have access to management information k) Provide support to the Buyer when the service encounters SIM or network issues to resolve issues quickly and reduce the impact to users l) Liaise with the End User requestor to ensure service fulfilment is completed to agreed performance indicators	**Must**	[redacted]	
MBS.002	**Digital Workplace**	**Mobile Service**	The Supplier must collaborate with Buyer's SIM (including but not limited to E-SIM) third party providers in the provision, maintenance and support of Buyer Devices. Specifically in identifying the root cause of any service issue and ensuring the responsible supplier is identified and tasked with a timely resolution in line with contracted levels or best industry standards if there is no applicable contracted standard to apply.	**Must**		