

Statement of Requirement (SoR)

For: Business consultancy Corporate Procurement

Reference Number	RQ0000044168
Version Number	0.1
Date	28/09/2023

1.	Requirement
1.1	Title
	RM6273 – Employee Benefits & Services
1.2	Summary
	<p>Dstl to offer a complete benefits package.</p> <p>Fully Managed benefits package (Lot 1) which includes:</p> <ul style="list-style-type: none"> • [REDACTED] ■ [REDACTED]

	<p>This would provide employees with access through one service provider who can offer both value for money and an excellent level of service whilst meeting our security and digital requirements.</p>
<p>1.3</p>	<p>Background</p>
	<p>The Defence, Science and Technology Laboratory (Dstl) employees over 5300 civil servants, a highly skilled and professional workforce largely comprised of scientists, engineering and analysts.</p> <p>Engagement on pay and benefits is low with only [REDACTED] of the workforce satisfied with pay and benefits despite the benefits being competitive.</p> <p>Dstl's employees are predominately based in [REDACTED]</p> <p>Dstl has a comprehensive benefits package, similar to that of many Other Government Departments and is seeking ways to modernise the offer in order to build on and develop in the future. Current benefits Dstl offer include:</p> <ul style="list-style-type: none"> • [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED] ■ [REDACTED]
<p>1.4</p>	<p>Requirement</p>
	<p>We would expect a contract to last from May 2024 to May 2027 for a period of 3 years with the option to extend by 6 months and an agreed notice period for both parties.</p> <p>We would want a designated Account Manager with whom we have regular (monthly) contact/access and with whom we agree a Service Level Agreement. This would include monthly reporting, system updates, identified errors and issues, marketing updates and details of ongoing promotions with potential to offer on-site promotion. Notification of any ad hoc employee communications prior to them being issued to the employee. Notification</p>

	<p>of and finance issues relating to non-payment of invoices that would affect the service being provided.</p> <p>Agree a timeline for implementation and/or agreed changes.</p> <p>All employees should be able to access a digital platform to access the benefits using their works email address, employee staff number and name.</p> <p>Technical support to be provided to Dstl account holders 24/7 i.e for the administration/set up in the site and also to individual users with a contactable customer services team (phone and/or email) who can resolve issues.</p> <p>Maintenance of site, limiting downtime, providing stringent security and notice of any service disruption to users in advance of planned maintenance.</p> <p>Safe processing of data, provision of MI and data reports where appropriate to Dstl and resolution and reporting and reporting of any breaches and security concerns.</p>
<p>1.5</p>	<p>Options or follow on work</p>
	<p><i>Not applicable</i></p>

1.6 Deliverables & Intellectual Property Rights (IPR)						
Ref.	Title	Due by	Format	Expected classification (subject to change)	What information is required in the deliverable	IPR DEFCON/ Condition
D1	Monthly Report	Monthly	Word doc. / Excel file	OFFICIAL/ OFFICIAL SENSITIVE	A pack summarising site usage and relevant statistics related to member activity through the platform. Information on spend and savings along with details around which benefits are being used.	N/A
D2	Account Management Meeting	Monthly/Quarterly	F2F/Video Call	OFFICIAL/ OFFICIAL SENSITIVE	Overview of relevant information for the fully managed service. Performance against KPIs and troubleshooting of issues.	N/A

1.7	Deliverable Acceptance Criteria
	<p>Implementation of Reward Portal/Website as a single point of entry for staff to use rewards and services. Access should be through a secure admin portal customised and branded to Dstl. .</p> <p>Adherence to relevant GDPR and data processing legislation with the swift reporting of issues including loss of information or data breach.</p>

2.	Quality Control and Assurance
2.1	Quality Control and Quality Assurance processes and standards that must be met by the contractor
	<p><input checked="" type="checkbox"/> ISO9001 (Quality Management Systems)</p> <p><input checked="" type="checkbox"/> ISO14001 (Environment Management Systems)</p> <p><input type="checkbox"/> ISO12207 (Systems and software engineering — software life cycle)</p> <p><input type="checkbox"/> TickITPlus (Integrated approach to software and IT development)</p> <p><input checked="" type="checkbox"/> Other: (Please specify below)</p> <p>Cyber Essentials Plus</p> <p>ISO 27001:2013 (International Standard for information security)</p> <p>ISO 22301:2019 Business Continuity Management</p> <p>ISO 14001:2015 Environmental Management</p>
2.2	Safety, Environmental, Social, Ethical, Regulatory or Legislative aspects of the requirement
	<p>GDPR legislation for the handling and processing of data, reporting of breaches and loss of information and ability to make data requests.</p>

3.	Security	
3.1	Highest security classification	
	Of the work	OFFICIAL SENSITIVE
	Of the Deliverables/ Output	OFFICIAL SENSITIVE
3.2	Security Aspects Letter (SAL)	
	Yes If yes, please see SAL reference- RQ0000044168	
3.3	Cyber Risk Level	
	Moderate	
3.4	Cyber Risk Assessment (RA) Reference	
	RAR-779010472 If stated, this must be completed by the contractor before a contract can be awarded. In accordance with the Supplier Cyber Protection Risk Assessment (RA) Workflow please complete the Cyber Risk Assessment available here	

4.	Government Furnished Assets (GFA)
GFA to be Issued - Supplier to specify	

5.	Proposal Evaluation criteria
5.1	Technical Evaluation Criteria
	Please refer to the evaluation guidance document and social evaluation annex A.
5.2	Commercial Evaluation Criteria
	Please refer to the evaluation guidance document.

6.	Defcons
Defcon:	Covering:
531	Disclosure of Information
532B	Protection of Personal Data
539	Transparency
658	Cyber
Deforms:	
532	Personal Data Particulars
539A	Tenderer's Sensitive Information