

Appendix F - Specification

This document sets out the Council's requirements, quality standards and key performance indicators with respect to the proposed contract. Please ensure that you read this carefully and ensure these requirements are incorporated into your pricing submission and the quality of services provided.

1. Council's Requirements

To have in place a contract for retained hours of service with a provider of specialists with the specific forensic ability to assess, mitigate and resolve issues arising from an identified cyber-attack or security breach on Lambeth in line with identified processes, policies and procedures.

The council are seeking a single supplier for a 24x7x365 service which provides a rapid response from subject matter experts (SMEs) in the event that we report a cyber-attack or security breach to them through an agreed method of contact.

Suppliers are invited to submit a proposal which defines how and what subject matter expertise would be provided within 1 hour of our request on a 24x7x365 basis. Furthermore, suppliers are invited to explain exactly what this service will incorporate, including its content, duration and how continuity would be achieved if the service is required over a long period of time.

The proposal must include provision for the onboarding process which is to include a gap analysis, including the creation of processes, procedures, playbooks and creation of an incident response plan as outlined in Appendix B – Instructions for Quotation Table 1 criteria 4.

A guaranteed SME response time is most important to the council but, if the supplier is unable to guarantee an SME response of 1 hour on a 24x7x365 basis, then we will consider alternative proposals that meet quality and service continuity criteria.

The council will have the ability to call upon these services through an agreed single point of contact from the commencement date of the 12-month contract with the supplier.

2. Insurance Requirements

The successfully appointed supplier should meet all insurance requirements as per Appendix E – Contract terms and conditions:

- Employers liability
- Public liability
- Professional indemnity cover

3. Quality Standards

The successfully appointed supplier must meet all requisite quality standards such as ISO 27000, ISO 27001, ISO 27035 or NIST.

A copy of the certification must be submitted by the provider as part of this tender.

4. Experience

The successfully appointed supplier will have demonstrable experience and certifications that they have achieved to be considered as a subject matter expert in the field of cyber resilience. References should be available on request as laid out in Appendix B, Table 1, Criteria 3.

Appendix F - Specification

5. Key Performance Indicators

The key performance indicators of this contract are:

- The supplier responds to activation within an hour of contact 24/7/365, deploying SME to assist in the response, mitigation and recovery of the perceived/received cyber-attack or security breach
- The supplier provides a post incident report to the Council with detailed activities and suggestions for remediation actions moving forward, within 10 days of the incident being closed
- The supplier provides first responder training to key Lambeth staff, along with regular testing of existing incident response plans and procedures to ensure a high level of resilience to cyber-attack or security breach whilst enhancing Lambeth cyber threat maturity

The supplier will present an initial plan for meeting these requirements at contract commencement and will report on a quarterly basis on the progress against each of these KPIs.

6. Frequency of Contract Meetings

- The supplier will report to Gerry Cast gcast@lambeth.gov.uk and George Ratcliffe gratcliffe@lambeth.gov.uk
- As per Appendix D - Delivery milestones, a briefing meeting will occur between the successful tendered and the Authority on w/c 29th November 2021
- The supplier will meet with all key Lambeth personnel on a monthly basis for the first three months, with a view to decrease regularity to quarterly meetings for review, or after every attack is successfully mitigated to debrief on activities conducted and identify key lessons learnt.
- There will be quarterly meetings between the Authority and the supplier in **March, June, September** and **December** in the contract year. Meetings will be held online – on Microsoft Teams or Skype – unless agreed by both parties in writing. Dates and timings will be agreed by both parties at the start of the contract.

We anticipate discussing the following agenda at each meeting:

- Review of the performance of the contract to date in relation to the KPIs
- The monthly reports covering the progress made in regard to onboarding, provision of training and upcoming penetration testing or tabletop exercises
- Any post incident reports with lessons learnt in the previous quarter
- Any issues experienced by the provider or by the Authority
- Any other business

7. Contract Management Arrangements

- The supplier must submit monthly reports, in PDF format, on the first Friday of each month, to Gerry Cast gcast@lambeth.gov.uk
- The reports must cover the following items:
 - Onboarding progress/activations of service
 - Training provision planned or delivered
 - Penetration testing planned or delivered
 - Tabletop exercises planned or delivered