**Appendix D – Response to Section 3**

|  |
| --- |
| 3.1 The National Archives requires a resilient, cloud-based software as a service solution that provides a fully integrated unified communications platform including video and voice conferencing, messaging, chat and enterprise telephony with global PSTN connectivity, using Microsoft Teams as a single unified communications client.  |
|  |
| 3.2 The solutions provider must include provision in its pricing to design, customise, configure and commission the system |
|  |
| 3.3 The solution must support our use of on-site analogue emergency phones and DECT analogue infrastructure |
|  |
| 3.4 The solutions provider must offer a self-service centralised management and administration console for administration of all services |
|  |
| 3.5 There must be full integration with Microsoft Active Directory for administration of users with support for single sign-on Active Directory Federation Services |
|  |
| 3.6 There must be a fully integrated virtual contact centre, delivering all aspects of contact centre management |
|  |
| 3.7 Provide a telephone call package with at least 45,000 inclusive minutes per month to UK national landline and mobile networks |
|  |
| 3.8 Provide for an optional International telephone call package of 500 minutes per month inclusive of all calls to international destination landlines |
|  |
| 3.9 Ideally the solution will incorporate a web chat facility. We require an independent but integrated live web chat system that can be delivered via our website through the virtual contact centre |
|  |
| 3.10 The solutions provider must declare whether The National Archives requires any third party licences for their solution to operate, e.g. Microsoft E5 licences or Microsoft telephony add-on services |
|  |
| 3.11 The solutions provider must declare whether any bots need downloading to the Microsoft Teams bot framework |
|  |
| 3.12 Train the trainer and administrator training in the use of the supplier’s solution must be included |
|  |
| 3.13 The solution must have full resiliency with a robust architecture offering at least 99.99% service availability with complete redundancy |
|  |
| 3.14 The supplier must demonstrate good information security governance and practices, typically through externally validated accreditation of policies and practices against recognised standards, e.g. Cyber Essentials Plus, ISO 27001 (see section 4 for more information on information security) |
|  |
| 3.15 The supplier should follow the best practice requirements for sensitive data and must provide a description of how they meet the best practice measures |
|  |
| 3.16 Ideally the supplier will demonstrate compliance with NCSC’s Cloud Security Principles and must describe in their response what they do that follows this guidance <https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles> |
|  |
| 3.17 Service Levels |
|  |
| 5.5 **Confirmation** that you are able to meet the requirements described in Sections 3 & 4 of the ITT |
|  |