**APPENDIX C**

**Information Assurance - DATA Security Questionnaire v5.3 Updated: August 2022**

|  |  |  |  |
| --- | --- | --- | --- |
| **8.3 Data Protection and Information Security Assurance Questionnaire – Pass / Fail**  *Please refer to:* <https://ico.org.uk> *for further information.*  *Other useful information can be found on this website:* [National Cyber Security Centre - NCSC.GOV.UK](https://www.ncsc.gov.uk/) | | | |
| **Question** | | **Pass/Fail Criteria** | **Response** |
| **8.3.1** | What is your ICO Registration or Fee Payers Number? (As per):  <https://ico.org.uk/ESDWebPages/Search> | **Pass:** A Valid Registration or Fee Payers Number or an Exemption Letter from the ICO provided in response  **Fail:** No Registration, Fee Payers Number or exemption letter is provided, or invalid number is provided in response | Insert ICO Registration, Fee Payers Number or explanation: |
| **8.3.2** | Have you had a security breach resulting in loss of or damage to personal or confidential information within the past 2 years? | **Pass:** Response is ‘No’ or Response is ‘Yes’ and sufficient details are provided stating what measures have been taken to avoid re-occurrence  **Fail:** Response is ‘Yes’ but no details provided to state what measures have been taken to avoid re-occurrence | Yes  No |
| If **YES**, please provide details and state the measures that have been taken to avoid re-occurrence here: | | |
| **8.3.3** | Have you had a security breach resulting in unauthorised disclosure of personal information within the last 2 years?  If **YES**, please provide details and state what measures have been taken to avoid re-occurrence | **Pass:** Response is ‘No’ or Response is ‘Yes’ and sufficient details are provided stating what measures have been taken to avoid re-occurrence  **Fail:** Response is ‘Yes’ but no details provided to state what measures have been taken to avoid re-occurrence | Yes  No |
| If **YES**, please provide details and state the measures that have been taken to avoid re-occurrence here: | | |
| **8.3.4** | Have you been the subject of any complaints to the Information Commissioner within the past 2 years?  If **YES**, please provide details and state what measures have been taken as a result | **Pass:** Response is ‘No’ or Response is ‘Yes’ and sufficient details are provided stating what measures have been taken to avoid re-occurrence  **Fail:** Response is ‘Yes’ but no details provided to state what measures have been taken to avoid re-occurrence | Yes  No |
| If **YES**, please provide details and state the measures that have been taken to avoid re-occurrence here: | | |
| **8.3.5** | **Data Processors checklist**  Designed to help you, as a processor, understand and assess your high-level compliance with data protection legislation. It includes the requirements for processors, the rights of individuals and data breaches under the General Data Protection Regulations.  **If you are working as our Data Processor** you will need to complete the Information Commissioner’s Office Data Processors checklist and forward the results  <https://ico.org.uk/for-organisations/data-protection-self-assessment/processors-checklist/>  **OR**  **If you are working as a Data Controller** you will need to complete the Information Commissioner’s Office Data Controllers checklist and forward us the results  <https://ico.org.uk/for-organisations/data-protection-self-assessment/controllers-checklist/>  Confirm you have attached the relevant ICO Data Protection checklist | **Pass:** Checklist response is rated as ‘GREEN’, or an ‘AMBER’ rating where sufficient clarification is received  **Fail:** Checklist response is ‘RED’ | Relevant checklist is attached:  Yes  *Organisations must attach the ICO checklist self-assessment, showing the outcome and also associated evidence to confirm assurances (e.g. copies of any certifications etc.)* |
| **8.3.6** | **Information Security Questions Part 1**  Complete the “Information Security” assessment, via the online link below. Once completed, download the assessment and please return this with this questionnaire for evaluation.  **Information Security**  This assesses your compliance with data protection in the specific areas of information and cyber security policy and risk, mobile and home working, removable media, access controls and malware protection  <https://ico.org.uk/for-organisations/data-protection-self-assessment/information-security-checklist/>  Confirm you have attached the ICO Information Security checklist  **YES / NO** | **Pass:** Checklist response is ‘rated as ‘GREEN’, or an ‘AMBER’ rating where sufficient clarification is received  **Fail:** Checklist response is ‘RED’ | Checklist is attached:  Yes |
| **8.3.7** | **Information Security Questions Part 2 – ICT systems ONLY**  See **APPENDIX D**  **This questionnaire will require completion by the winning bidder ONLY** |  |  |

**PLEASE COMPLETE**

|  |  |
| --- | --- |
| Contact details and declaration | |
| Question | Response |
| Contact name |  |
| Name of organisation |  |
| Role in organisation |  |
| Phone number |  |
| E-mail address |  |
| Postal address |  |
| Signature (electronic is acceptable) |  |
| Date |  |

*Instructions for Completion*

The purpose of this questionnaire is to assist Cheshire East Council in deciding which suppliers can provide the necessary assurances around confidentiality, integrity and availability.

1. In order to provide a full evaluation and the necessary assurances for this process, suppliers should provide any supporting documents, for example, certificates, statements or policies with this questionnaire. You may also be asked to clarify your answers or provide more details.
2. This questionnaire must be responded to in full even if your organisation has previously submitted a questionnaire to the Council. It is not sufficient to refer to earlier or other questionnaires.

***By completing the questionnaire, you confirm the information is correct and accurately reflects processes and procedures adopted within the organisation.***

1. Any questions answered incorrectly with the sole purpose of deception, will be seen as fraudulent activity, and reported accordingly.
2. Suppliers not currently registered in the UK should answer all questions substituting where relevant the appropriate professional or commercial registers, legislation, Codes of Practice etc., which are applicable within their domestic jurisdiction.
3. The information disclosed in this questionnaire will be used as part of the selection criteria for awarding contracts
4. Unless instructed otherwise, please complete the form on behalf of the Organisation applying for the tender. If your organisation is part of a group of Companies, this submission should represent the organisation applying for the tender and not the Group
5. The supplier can and should provide any security whitepapers, technical documents, or copies of policies as necessary to fully demonstrate compliance with the requirements.

***All questions and comments within the questionnaire are mandatory unless they are not applicable.***

1. The supplier must clearly explain why a given question is not applicable.
2. For all other questions, if a requirement cannot be met, the supplier still has an opportunity to meet the requirement by the use of compensating controls. Compensating controls must be described in full. In such circumstances, the supplier must provide a full explanation of the compensating control including an explanation of how the control meets the intent of the original question. Cheshire East Council has the sole right to determine if a proposed compensating control is an acceptable solution.
3. Cheshire East Council has the sole right to determine if the details provided describe a solution that truly meets or exceeds the needs of Cheshire East Council.
4. As part of the selection process suppliers must demonstrate compliance with the criteria within the questionnaire by responding to every relevant statement and question. Validation of the responses provided by the supplier will be conducted during the evaluation and audit process. Any erroneous information could limit the supplier's ability to finalise implementation of the proposed solution.
5. Suppliers are expected to maintain an awareness of the laws and regulations applicable to the use of the proposed solution in a Local Authority environment. Including the DPA (Data Protection Act) 2018 and GDPR (General Data Protection Regulation) 2016.