*APPENDIX D*

# Information Security Assessment

[Name of procurement]

The table below is to be completed by the service seeking to undertake the procurement activity in question. The information provided in this table will help inform the results of the final risk assessment.

| |
|---|
| **1) Name of company** |
| |
| **2) Contract reference number** |
| |
| **3) Name of contract** |
| |
| **4) Contract description** |
| |
| **5) Is personal data to be processed as part of this contract** |
| |
| **6) If you answered "Yes" to question 5, please describe the processing of personal data which takes place (This should be a high level, short description of what the processing is about i.e. its subject matter)** |
| |
| **7) If you answered "Yes" to question 5, please state the duration of this processing (clearly outline any relevant dates).** |
| |
| **8) If you answered "Yes" to question 5, please describe the nature of the processing. (The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means)** |
| |
| **9) If you answered "Yes" to question 5, please state the type of personal data. (Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc)** |
| |
| **10) If you answered "Yes" to question 5, please describe the categories of personal data you process. Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc.** |
| |
| **11) If you answered "Yes" to question 5, please outline your plan for return and or destruction of the personal data once the processing is complete. If your contract states you will retain the data please state this. Describe how long the data will be retained for, how it be returned or destroyed.** |
| |

Devon County Council has a legal requirement to ensure that the personal data we are responsible for is kept secure. To enable us to comply with this requirement, Devon County Council must ensure that any person (whether individually or on behalf of an organisation) processing personal data on the Council's behalf (a data processor) can provide sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out and take reasonable steps to ensure compliance with those measures.

Any data processor who has access (directly or indirectly) to personal data held by the Council must complete this questionnaire and where directed, provide evidence showing how they meet the necessary security standards for protecting personal data against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Persons processing data on behalf of the Council which will not have access to personal data (a third party), may still be required to complete this questionnaire if they have access to sensitive business information or business critical systems.

Instructions to data processors and third parties;

1. This questionnaire must be completed by the individual responsible for Information Security within the company or business tendering for the work being contracted out by Devon County Council.

2. This questionnaire consists of two columns; the first column lists the security questions and the second column requires the data processor or third party to provide their response to the questions. Data Processors and third parties must not modify or delete any questions. If the question does not apply to the services or work that is to be provided, then an "N/A" (not applicable) in the response column is sufficient.

3. Please complete this questionnaire as fully as possible and provide as much information as you are able to. Incomplete or partial answers may result in additional questions and can delay the process. Once the form has been completed, return it to the designated project lead involved in this contract.

- **Name of Bidder**: [bidder name]
- **Evaluated by (IG)**: [officer name]
- **Evaluated by (ICT)**: [officer name]
- **Outcome**: [Adequate Assurance/ Progressed through Information Risk Assessment]

| | |
|---|---|
| **1.0 General information**<br>***Overview of section***<br>Devon County Council requires general information about your company. | |

| | |
|---|---|
| 1.1 What is the project name? | |
| 1.2 Please describe the project and the work that is being contracted out. | |
| 1.3 What is the name, email address and telephone number of Devon County Council's lead for this project? | |

| | |
|---|---|
| 1.4 What is the name and telephone number of your company? | |
| 1.5 What is your company's postal address? If this is different to where the service or work for Devon County Council would be carried out, please include this address also. | |
| 1.6 Does your company own or manage this environment or premises? If not, please identify who does? | |
| 1.7 What is your company's website address? | |
| 1.8 What is the name, email address and telephone number of your company's Information Security or Data Protection Manager or security lead? | |

| | |
|---|---|
| 1.9 Is your company registered under the Data Protection Legislation, with the Information Commissioner's Office?<br>If yes, what is your registration number?<br>If no, please explain why not. | |
| 1.10 Is your company certified under the Information Security Standard ISO27001or accredited to any other security related standard or Code? If yes, please provide details. | |
| 1.11 Describe the type of information or data your company would be processing on behalf of Devon County Council. | |
| 1.12 Will your company be processing personal or sensitive data on behalf of Devon County Council? | |

| | |
|---|---|
| 1.13. Will your company be subcontracting any of the work being tendered for? If yes, please provide full details and confirm that authorization has been given by DCC.<br><br>*(NB. Subcontracting is prohibited unless Devon County Council has explicitly authorized this. Subcontractors may be required to complete this questionnaire).* | |
| **2.0 Human Resources Security**<br>***Overview of section***<br>Devon County Council requires that all individuals who have access to its data are appropriate and trustworthy and are only given access on a strict need to know basis. The Council prohibits the disclosure or distribution of its information to any other third party or data processor, unless explicitly authorized. | |

| | |
|---|---|
| 2.1 How many employees does your company have? | |
| 2.2 Please provide details of the background checks your company carries out on new staff or contractors to ensure their reliability and trustworthiness. | |
| 2.3 Please provide a copy of the Data Protection and/or confidentiality clauses included in staff contracts. | |
| 2.4 Please provide details of the information security or data protection training your company provides to its staff.<br>Please include a copy of the training materials. | |

| | |
|---|---|
| 2.5 Is information security or data protection training mandatory for your staff and how often is the training provided?<br>If the training is not mandatory for all staff then please explain why not? | |
| 2.6 Please provide details of any incidents involving the loss, misuse or theft of any personal or business sensitive information by your staff in the last 3 years. | |
| 2.7 Has your company self reported any information security incidents to the Information Commissioner's Office or been reported to the Information Commissioner's Office regarding information security incidents in the last 3 years? If so, please describe the incident(s) and the outcome. | |

| | |
|---|---|
| **3.0 Policy and awareness**<br>***Overview of section***<br>Devon County Council expects your company to have a formal data protection and/or information security Policy, outlining the measures your company takes to protect personal data and or sensitive business data. | |
| 3.1 Please provide a copy of your company policy (or policies) which refers to information security and data protection. | |
| 3.2 Please provide details of how your company promotes awareness of these policies to staff and contractors and any formal training and sign off required. | |

| | |
|---|---|
| 3.3 Please provide details of your company's policy for dealing with Freedom of Information or Subject Access requests that would require the disclosure of Devon County Council data. | |
| 3.4 Please provide details of your company's policy with regard to Data Retention and Data Destruction. | |
| **4.0 Physical security**<br>***Overview of section***<br>Access to Devon County Council data must be strictly controlled. All data processing devices holding the Council's data must be held in secure rooms with controlled access. Access to physical media and documentation must also be controlled and must always be held in locked storage when not attended. | |

| | |
|---|---|
| 4.1 Describe the physical and electronic security measures used to protect Devon County Council's information on the premises where the information would be held. | |
| 4.2 If the information or data is to be held electronically, where will the data back ups be held and what physical and electronic security will be used to secure them? | |
| 4.3 If requested, can a representative from Devon County Council visit the company's facilities to observe the physical security controls in place (announced or unannounced)? | |

| | |
|---|---|
| **5.0 Technical controls**<br>***Overview of section***<br>Devon County Council requires companies and other persons to have appropriate technical measures in place to protect the Council's personal data and sensitive business data, from unauthorized or unlawful processing and against accidental loss or destruction of or damage to the data. | |
| ***Segregation of Information between Clients***<br>5.1 Please provide details of the security controls in place to keep Devon County Council systems and data separate from that held on behalf of your company's other clients. | |
| ***Operating System Security***<br>5.2 Please provide details of the Information Security procedures your company uses for protecting its systems against vulnerabilities. | |

| | |
|---|---|
| 5.3 Please provide details of the routine vulnerability scanning your company performs of its customer environment and the system tools that are used? | |
| 5.4 What application security test reports for public facing internet based applications allowing access to Devon County Council data is your company able to provide? | |
| 5.5 What is your company's patch management process? | |
| 5.6 What anti-virus software does your company deploy on its systems and how often are virus definitions updated? | |

| | |
|---|---|
| ***Authentication and Authorization***<br>5.7 Please provide details of the secure encrypted protocols the company uses to manage servers and network devices. | |
| 5.8 What type of authentication is required to access servers and network devices, both from on-site and remote access (e.g. passwords, SecurID)? | |
| 5.9 How is access to the data/information the company would be processing on behalf of the Council controlled? How are duties segregated between staff? | |
| 5.10 Please describe the procedure and system requirements for company's employees to access its network remotely. | |

| | |
|---|---|
| ***Protection of Sensitive Data***<br>5.11 How is electronically held personal data and sensitive business information, protected from unauthorized or unlawful processing? | |
| 5.12 How is electronically held personal data protected against accidental loss, destruction or damage? | |
| 5.14 How will personal or sensitive business data be encrypted both in transit and in storage? Please describe key management practices and the encryption algorithms used. | |
| 5.15 Will your company be holding personal data, belonging to the Council, on its own server or on cloud servers? If yes, is your server or the cloud server held in the European Economic Area? If answering no, please provide details. | |

| | |
|---|---|
| ***Network Security***<br>5.16 Please provide details of the Firewall software that will be used to protect Devon County Council data and systems from the Internet and other untrusted networks, and the formal security accreditations they possess. | |
| 5.17 Please provide details of any intrusion detection/prevention systems used. | |
| 5.18 Please provide details of how frequently security logs are monitored to detect malicious activity. | |
| 5.19 Please provide details of how the company correlates security events from different sources. | |
| 5.20 Please provide details of any wireless technology that will be used and how it will be protected. | |

| | |
|---|---|
| **6.0 Organisation standards**<br>***Overview of section***<br>Devon County Council requires companies and other persons to have appropriate standards in place to protect its data. Security incidents must be reported to: KeepDevonsDataSafe@devon.gov.uk These include, but are not limited to, unauthorized access, denial of service, loss or theft of information and data corruption. | |

| | |
|---|---|
| 6.1 What is your company's process for disposing of sensitive written or printed material? | |
| 6.2 What is your company's process for disposing of computer equipment used in processing of data? | |
| 6.3 How often are permissions for access to written or printed material and access to computer systems (i.e. physical and logical access) periodically reviewed? | |
| 6.4 What methods would your company employ to verify a user's identity in respect of access to Devon County Council's data (this must include physical and logical access)? | |
| 6.5 What are your company's procedures for reporting security incidents to your clients? | |

***APPENDIX D TO BE READ IN CONJUNCTION WITH THE DATA PROTECTION POLICY***