Search Centre

|  |  |
| --- | --- |
| *Reference number* |  |
| *Approved by* | **Information Management and Technology Board** |
| *Date approved* | **2016** |
| *Version* | **1.1** |
| *Last revised* | **October 2018** |
| *Review date* | **June 2021** |
| *Category* | **Information Assurance** |
| *Owner* | **Data Protection Officer** |
| *Target audience* |  |

**HEREFORDSHIRE COUNCIL SUPPLIER SECURITY ASSESSMENT**

This is a **CONTROLLED** document and updates or changes to this document are authorised and then advised by email to the relevant document holders.

It is **UNCONTROLLED** when printed. You should verify that you have the most current issue

## INTRODUCTION

Herefordshire Council Information Security Policy requires an evaluation of third parties who process, handle or store information on behalf of them.

To assist us in meeting our data protection obligations, this questionnaire should be completed by the person responsible for Information Security within the organisation being contracted to provide services to Herefordshire Council.

This questionnaire consists of two columns, one with the question posed to you, the second for your response. You are not to modify or delete any of the questions. If the question does not apply to the services that are to be provided, then an “N/A” in the answer response column is sufficient.

Once the questionnaire is completed, it is to be returned to Information Governance [informationgovernance@herefordshire.gov.uk](mailto:informationgovernance@herefordshire.gov.uk)

Any questions should also be directed to [informationgovernance@herefordshire.gov.uk](mailto:informationgovernance@herefordshire.gov.uk)

## GENERAL INFORMATION

|  |  |  |
| --- | --- | --- |
|  | Company name and address |  |
|  | Your company’s website. |  |
|  | Information Security Contact (name and phone). |  |
|  | Who is your normal Contact with us? |  |
|  | How will you communicate changes in service to us? |  |
|  | How long have you been in the business of providing the service requested by us? |  |
|  | Number of employees. |  |
|  | Is your company registered with the UK’s Information Commissioner? If so please provide your notification number. |  |
|  | Have any independent 3rd party security reviews been performed on the organisation? If so, who performed the review and when was it performed? |  |
|  | Can you provide a copy of an independent 3rd party security audit relevant to the services Herefordshire Council will be subscribing? |  |
|  | What information will the organistation be processing, handling or storing on behalf of Herefordshire Council? If so, does this include personal details such as name and address? |  |
|  | At what address are the systems located that will be supporting our services? |  |
|  | Do you own/manage this environment? If not, please list who does. |  |
|  | Will you be subcontracting any work? |  |
|  | Are you certified to any information security or quality standards e.g. ISO 27001, ISO 90001 - if so please state the scope for these standards. |  |
|  | Does the software/system provided full audit trail functionality reporting on specific records viewed, created and updated, logs of access times and dates of user logons etc. |  |
|  | Will any Council data be hosted in the cloud?  If so what cyber security standards are you compliant with e.g. National Cyber Security Centre guidance – 14 Cloud Security Principles or the CSA Star Assessment? |  |

## POLICY & AWARENESS

|  |  |  |
| --- | --- | --- |
| 3.1 | Do you have a formal information security policy? If so, please provide a copy |  |
| 3.2 | Is the policy formally approved by senior management and regularly reviewed? |  |
| 3.3 | Who is responsible for monitoring compliance to the information security policy? Does this take place on an annual basis? |  |
| 3.4 | How do you promote awareness of the policy for both staff and contractors (is formal training and sign off required)? |  |
| 3.5 | Do you ensure that specific security training is provided regularly (at least annually) to your employees, contractors and temporary staff? |  |

## HUMAN RESOURCES SECURITY

|  |  |  |
| --- | --- | --- |
| 4.1 | Please describe the level of vetting you carry out on employees and third parties. |  |
| 4.2 | Are all personnel required to sign non-disclosure or confidentiality agreements? |  |
| 4.3 | What disciplinary process do you have to ensure that any intentional misuse of information is managed for employees or sub-contractors? |  |
| 4.4 | Describe the process in place when personnel leave in terms of retrieval of equipment or information and staff’s ongoing responsibilities regarding non-disclosure. |  |

## SUB-CONTRACTORS or SUB-PROCESSORS

|  |  |  |
| --- | --- | --- |
| 5.1 | Do you have prior written consent from Herefordshire Council for any information processing by sub-contractors? |  |
| 5.2 | Do you have a documented process for the selection and transfer of activity to sub-contractors? |  |
| 5.3 | Do you have agreements/contracts in place to ensure that data privacy and security arrangements continue to meet the council’s security requirements? |  |
| 5.4 | Do you audit the security of your sub-contractors? |  |
| 5.5 | Should the need arise would the council be allowed to conduct a security review? |  |

## PHYSICAL SECURITY

|  |  |  |
| --- | --- | --- |
| 6.1 | Describe the security controls protecting the location where the information is being stored (e.g. physical entry arrangements - locked server cages, guarded access, video monitoring, visitor access controls) |  |
| 6.2 | What physical access and authorisation controls do you have for sensitive areas (also include areas that aren’t data centres but which could store or hold sensitive data e.g. comms. rooms) |  |
| 6.3 | What controls do you implement to control physical access for external party support engineers? |  |
| 6.4 | What environmental controls do you have in place to prevent accidental loss of data, for example raised flooring, fire detection and suppression controls? |  |
| 6.5 | Can a representative from Herefordshire Council visit your facilities to observe the physical security controls in place? (announced or unannounced) |  |

## OPERATIONAL CONTROLS - CHANGE & INCIDENT MANAGEMENT

|  |  |  |
| --- | --- | --- |
| 7.1 | Are changes to any of your systems tested, reviewed and applied using a documented change management process? Please describe. |  |
| 7.2 | Do you have an incident management process that is documented, approved and monitored? |  |
| 7.3 | Do you have procedures for reporting incidents to your clients? If so, please describe. |  |
| 7.4 | Do you have a process for dealing with incidents that require forensic investigation? |  |

## RISK ASSESSMENT & ASSET MANAGEMENT

|  |  |  |
| --- | --- | --- |
| 8.1 | Do you undertake regular security risk assessments and take steps to mitigate the risks identified? Please describe process. |  |
| 8.2 | Do you maintain an inventory of assets? |  |
| 8.3 | Do you have a data/information classification process? |  |
| 8.4 | Is our information held or transported on data storage media encrypted and protected against corruption, loss or disclosure? Please describe your arrangements. |  |
| 8.5 | What procedures do you have for the handling and management of removable media and hard copy information in transit & storage? |  |
| 8.6 | What back up arrangements do you have in place? How are offsite backups secured? |  |
| 8.7 | What procedures and mechanisms do you use for controlling and disposing of paper documents containing sensitive data? |  |
| 8.8 | Does the secure destruction of redundant equipment and media include the secure erasure of information? Please describe process. |  |

## TECHNICAL CONTROLS

### Protecting our Data

|  |  |  |
| --- | --- | --- |
| 9.A.1 | What security controls are in place to keep Herefordshire Council data separate from other client data? |  |
| 9.A.2 | What security controls are in place to ensure only we and those authorised by us, can access our data? |  |
| 9.A.3 | How is our data protected at rest? |  |
| 9.A.4 | How is our data protected when transmitted across your network? |  |
| 9.A.5 | How is our data protected when transmitted across the internet? |  |
| 9.A.6 | How is the availability to our data protected so that it available when we need it? |  |
| 9.A.7 | If encryption is used please describe how access and availability of the keys are controlled? |  |
| 9.A.8 | What will happen to our data when we withdraw from the service? |  |
| 9.A.9 | How do you ensure that our or our customers’ data is not processed by you or a third party without consent? |  |

### Access Control

|  |  |  |
| --- | --- | --- |
| 9.B.1 | How often do you review user access to ensure that staff continue to only have the minimum access they require for their current job? |  |
| 9.B.2 | Do you perform regular audits on user access exceptions e.g. failed login attempts etc.? |  |
| 9.B.3 | Do staff have unique identifiers on all systems? |  |
| 9.B.4 | Please describe your Password Policy (length, construction, ageing, etc.)? |  |
| 9.B.5 | What system access auditing processes and facilities do you implement? |  |

### C. Authentication and Authorisation

|  |  |  |
| --- | --- | --- |
| 9.C.1 | Do you manage servers and network devices using secure encrypted protocols? |  |
| 9.C.2 | What type of authentication is required to access servers and network devices, both from on-site and remote access (e.g. passwords, SecurID)? |  |
| 9.C.3 | How is access controlled to the data/information (e.g. segregation of duties) you are processing, handling or storing on behalf of Herefordshire Council? |  |
| 9.C.4 | Can an employee in your company access your network remotely to work on our behalf? If so, please describe the controls in place. |  |

### Operating System Security

|  |  |  |
| --- | --- | --- |
| 9.D.1 | Do you have procedures for protecting your systems against vulnerabilities? |  |
| 9.D.2 | Do you perform routine vulnerability scanning of your customer environment? If so, what tools are used? |  |
| 9.D.3 | Do you have a patch management process? |  |
| 9.D.4 | Is anti-virus software deployed on systems and how often are virus definitions updated? |  |

### E. Network Security

|  |  |  |
| --- | --- | --- |
| 9.E.1 | Are firewalls used to protect council data and systems from the Internet and other untrusted networks? |  |
| 9.E.2 | Are intrusion detection/prevention systems used? |  |
| 9.E.3 | Are security logs monitored to detect malicious activity? |  |
| 9.E.4 | Do you correlate security events from different sources? |  |
| 9.E.5 | Will wireless technology be used in this environment? If so, how is this protected? |  |
| 9.E.6 | Is penetration testing carried out and if so how often? |  |

### F. Systems Development

|  |  |  |
| --- | --- | --- |
| 9.F.1 | Are development activities carried out in accordance with a formal methodology including definition of testing of security requirements? |  |
| 9.F.2 | Are development activities performed in a test environment (isolated from the live environment) and protected against disruption and disclosure of information? |  |
| 9.F.3 | Are all elements of your systems tested development phase before the system is promoted to the live environment? |  |
| 9.F.4 | Do you ensure that live data is not used within test environments? |  |
| 9.F.5 | For Web applications do your developers mitigate the Open Web Application Security Project’s Top Ten? |  |

## BUSINESS CONTINUITY MANAGEMENT

|  |  |  |
| --- | --- | --- |
| 10.1 | Do you have a Business Continuity Policy and Plan and how often is it tested? |  |
| 10.2 | What were the results of your last Business Continuity test and does your organisation have any known risks in this area? |  |
| 10.3 | Please describe how your business continuity plan will affect Herefordshire Council. |  |

## COMPLIANCE

|  |  |  |
| --- | --- | --- |
| 11.1 | Can you confirm that all services or systems processing our information are compliant with all relevant statutory, regulatory, contractual, copyright and intellectual property requirements? |  |
| 11.2 | Can you confirm that all Council information containing personal information will be handled in accordance with UK Data Protection legislation? |  |
| 11.3 | Will the council’s data be shared with any other establishments, organisations or third parties? |  |
| 11.3 | Please provide a list of countries where our data is likely to be processed and the safeguarding of privacy in place there. |  |
| 11.4 | If our data will be processed in multiple countries, describe the circumstance which may cause our data to be transferred. |  |
| 11.5 | Can you limit the replication of data to specific countries or territories? |  |
| 11.6 | Has the Information Commissioner issued any assessments against you or required an undertaking to be signed? (If yes please provide further information). Have you ever had to report a breach to the data commissioner? |  |
| 11.7 | Have internal or external auditors conducted a review of information security arrangements in the last 12 months? Can you detail any weaknesses or improvements identified? |  |
| 11.8 | Please describe the processes in place to ensure the ongoing monitoring of your information security arrangements. |  |

## DECLARATION

**Signed Undertaking**

This document is signed in acceptance that the signatory’s organisation, and any other organisations accessing []’s assets on behalf of the contractor, will comply with all requirements herein.

**Senior Officer(s) for the CONTRACTOR with responsibility for the secure handling of Herefordshire Council’s Information**.

|  |  |
| --- | --- |
| **Signed:** |  |
| **Print Name:** |  |
| **Position in Organisation:** |  |
| **Dated:** |  |

**END OF DOCUMENT**