Due Diligence Questions– IG and ICT

Responses to these questions must be to the satisfaction of the Council’s Senior Information Risk Owner / Data Protection Officer and in accordance with the requirements of the General Data Protection Regulation ((EU) 2016/679) and the Data Protection Act 2018, you may also be asked to complete and sign the Council’s 3rd Party ICT agreement and an Information Sharing Agreement.

***Please supply as much detail as possible in the Confirmation and Assurance statement. Insufficient detail may result in the submission being returned for further clarification.***

|  |  |  |
| --- | --- | --- |
|  | **Requirement** | **Confirmation & Assurance statement** |
| **Hosted solutions and servers** |
| 1 | The hosting solution will be based in the UK and be compliant with ISO 27001 for physical and virtual security. |  |
| 2 | All data will be managed and stored in compliance with current data protection legislation and Cyber legislation or Regulations. |  |
| 3 | You will maintain a failover hosting solution which also is compliant with ISO 27001 for all physical and virtual security. |  |
| 4 | You will ensure that Blackpool Council is notified of any changes to the location of hosting facilities with at least 90 days’ notice. |  |
| 5 | Any upload facilities used and network services within your hosted solution will always be maintained with a level of secure encryption to prevent any unauthorised access or hacking to take place. Any Cipher codes must be fully supported and not deprecated. |  |
| 6 | You will specify a secure and updated web browser for use with the product which is supported by the browser manufacture's latest security recommendations. Should the browser withdraw support for the recommended browser version you will provide a new secure and manufacturer supported recommendation. |  |
| 7 | All servers, network components, firmware, operating systems and software provided as part of the hosted solution will be kept up to date to the latest secure versions. Any security vulnerabilities identified by the manufacturers of such software/firmware and components will be patched and updated within 7 working days of the manufacture releasing new and updated versions of code to remove the vulnerability. |  |
| 8 | Where additional back-up services are used these are regularly tested, and any that require use of removable media have procedures in place to store this off-site. Please provide details of the testing routine. |  |
| 9 | Any device/s used for system administration of hosted services must* Be ‘Managed’ devices within an organisation (not home PCs);
* Have up-to-date Anti-Virus installed;
* Have appropriate Firewall controls configured;
* Receive regular OS updates (Patches, Security updates etc.,)
* Using fully supported operating system in which the OS provider still provides regular security updates for to address emerging vulnerabilities
* Have Endpoint detection and security software installed on the machine to ensure that security and patching requirements are fully up-to-date where appropriate.
* Regularly scanned for vulnerabilities
 |  |
| 10 | The Supplier must enforce adequate security and authentication procedures for access to controlled data managed on behalf of the council and for the physical security of this data for which the Supplier is contractually bound. The Council must also be satisfied that backup and recovery procedures are appropriate and applied correctly. |  |
| 11 | Once the contract has ended or equipment has become obsolete or irreparable all Council data will be securely removed from all devices and systems so it unrecoverable. |  |
| 12 | The supplier will carry regular vulnerability scanning of the all hosted components and system admin devices and install critical updates within 7 working days.  |  |
| 13 | The supplier will maintain security logs and audit trails of all access to the hosted environment and record any copying or removal of data. These security logs will be made available to the Council or its appointed Cyber forensics specialists for investigation in the event of a breach/suspected breach of the Council’s data. |  |
| 14 | At least once every 12 months The Supplier will have the security of the hosted solution and system admin systems independently penetration tested for vulnerabilities by a CHECK certified consultant. Any critical vulnerabilities identified by such testing will be addressed within 7 days of the security report. In the event of a breach or suspected breach of the Council’s data this report will be made available to the Council or its appointed Cyber forensics specialist. |  |
| **Information Governance** |
| 15 | Please list the date of your registration with the Information Commissioner’s Office and the name the registration is made under. |  |
| 16 | Should the contract or service be terminated all copies of data transmitted and stored from Blackpool Council will be destroyed and disposed in accordance with the ISO 27001 standards unless otherwise specified in the contract. |  |
| 17 | At the end of the contract, all copies of data transmitted and stored from Blackpool Council will be returned to Blackpool Council or will be destroyed and disposed in accordance with the ISO 27001 standards as agreed in the contract specification. |  |
| 18 | Please detail all measures in place to restrict unauthorised or unnecessary access to information. |  |
| 19 | Please confirm that the use of removable media and paper records is restricted. Where removable media is used, this will be encrypted. |  |
| 20 | Secure transfers will be undertaken using agreed protocols |  |
| 21 | Your third party sub-contractors will only be authorised by Blackpool Council following your submission of statements that prove you have assessed their adherence to the technical and organisational measures required for current data protection legislation. |  |
| 22 | You and your third party sub-contractors should at all times comply with Blackpool Council's ICT Security and Data Protection Policies, and will be required to report any breaches to Blackpool Council's Data Protection Officer without undue delay from the date and time of discovery. |  |
| 23 | As a consequence you will be required to take any necessary steps required by Blackpool Council's Senior Information Risk Officer and Data Protection Officer to prevent any further breaches or actions required by regulatory bodies such as Information Commissioner. |  |
| **Premises Security (relating to the location of where the data is collected or processed)** |
| 24 | All entrances and exits to your offices should be controlled or on lock/keypad locks. |  |
|  | Only authorised staff have access to the data processing areas and measures are in place to restrict access and monitor this. |  |
| 25 | The processing workstations cannot be seen from windows or public areas. |  |
| 26 | Premises are protected by CCTV / Security / other means. |  |
| **People and Policy** |
| 27 | Your staff are aware of their responsibilities for data protection and confidentiality. |  |
| 28 | Your staff are trained in data protection and information/cyber security |  |
| 29 | You have data protection, and information/cyber security policies and procedures in place. |  |
| 30 | The Supplier will ensure its employees/subcontractors have all been cleared to a minimum of HMG Baseline Personnel Security Standards (BPSS). |  |