

Due Diligence Questions– IG and ICT

This document is intended to provide Blackpool Council with assurance that third parties implement appropriate technical and organisational measures to protect Council data, thus complying with the requirements of the Data Protection Act 2018 and UK GDPR. These questions must be to the satisfaction of both the Council’s Senior Information Risk Owner (SIRO) and Data Protection Officer (DPO), who reserve the right not to award should it be apparent that the solution offered would not protect the Council from risk.

Third parties 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** |
| 13 | Please confirm whether you are registered with the ICO and provide the following information: * The organisation name the registration is under
* Registration number
* Date of Expiry
 |  |
| 14 | Please confirm the name and contact details of your organisation’s Data Protection Officer Or confirm you do not have one. |  |
| 15 | Please provide **a copy** of your organisations data protection policy or equivalent. Please **list** any other data protection and information/cyber security policies or procedures the organisation has to support their core policy. |  |
| 16 | Please confirm and describe any data protection and information/cyber security training your employees routinely receive. |  |
| 17 | Please confirm that at the end or termination of the contract, whether copies of data transmitted and stored for Blackpool Council will be either: * returned to Blackpool Council without the Council incurring fees.
* Or will be destroyed and disposed in accordance with the ISO 27001 standards.

*\*Unless you are legally required to retain in which case please explain.* |  |
| 18 | Please describe measures in place to restrict unauthorised or unnecessary access to information. |  |
| 19 | Please confirm your organisation’s policy on removable media And if it is permitted whether it will be encrypted. |  |
| 20 | As part of delivery for this contract please confirm whether your organisation is required to use hard copies of any data processed or received by Blackpool CouncilAnd if so describe any measures to mitigate the risk of a data breach |  |
| 21 | Please confirm secure electronic transfers will be undertaken using agreed protocols |  |
| 22 | Please confirm whether you use any sub processorsAnd if so confirm third party sub-contractors will only be authorised following your submission of statements that prove you have assessed their adherence to the technical and organisational measures required for current data protection legislation. |  |
| 23 | Please provide **a copy** of your data breach procedure (or equivalent) Or in the absence of a formal procedure provide a summary of your breach management process. Please confirm the timeframe for notifying the Council of a breach |  |
| 24 | In the event of a breach of the Council’s data please confirm you will take 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)** |
| 25 | Please confirm entrances and exits to your offices are controlled or on lock/keypad locks. |  |
| 26 | Please confirm only authorised staff have access to the data processing areas and describe any measures in place to restrict and monitor access  |  |
| 27 | Please confirm that processing workstations cannot be seen from windows or public areas. |  |
| 28 | Please confirm whether a CCTV is placeAnd describe any additional security measures. |  |

|  |
| --- |
| **If Applicable** |
| 29 | Please confirm employees/subcontractors have all been cleared to a minimum of HMG Baseline Personnel Security Standards (BPSS).Or confirm this is not applicable |  |