**Cheshire East Council ICT Security Hosted Procurement Questionnaire**

As part of the selection process Suppliers must demonstrate compliance with the security criteria listed by responding in writing to every relevant statement and question. Validation of the answers provided by the supplier may be conducted during the review/audit process. Any erroneous information could limit the vendor's ability to finalise implementation of the proposed solution.

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.

**Documentation**

The Supplier should provide security whitepapers, technical documents, or copies of policies as necessary to fully demonstrate compliance with the requirement. Failure to provide the necessary information to meet the requirements in this section could lead to potential disqualification.

**Compensating Controls and Descriptions**

All statements and questions below are mandatory unless they are not applicable. The Supplier must clearly explain why a given question is not applicable. 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. When more room is needed to fully explain the compensating control, attachments can be included in the response so long as such attachments are labelled and cross-referenced in the response. 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.

In some instances, Cheshire East Council has requested that the Supplier provide a description to accompany their response to a particular statement or question below. Descriptions are requested when an answer alone could be deceptive without further detail. When more room is needed to provide a complete description, attachments can be included in the response so long as such attachments are labelled accordingly. 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.

***Suppliers/Product Information (MUST BE COMPLETED)***

**Suppliers Name and Contact Information:**

**Product Name and Brief Description:**

Supplier represents and warrants that their responses to the questions are accurate and that the system configuration will continue to conform to these answers unless mutually agreed upon by Cheshire East Council and the Supplier. Supplier further agrees to work with Cheshire East Council in good faith to maintain compliance with new laws and regulations and/or to improve the security of the system.

Agreed this \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ day of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 20\_\_

Company Name

Signer's Name

Signer's Title

**Cheshire East Council ICT Security**

**Instruction:**

1. The work limit for your response to each question is 500.
2. Diagrams and pictures can be used in your response.

|  |  |  |
| --- | --- | --- |
| **Ref** | **Requirements** | **500 word maximum for your written response.** |
| **1** | **ICT Security and Data Protection** |  |
| **1.01** | **Governance** | **Response** |
| 1.01.1 | Please provide full contact details of your appointed Senior responsible named officer, associated personnel and resources who will act as a first point of contact and conduct ongoing management of security incidents including identification, managing and agreed reporting procedures for actual or suspected security breaches. |  |
| 1.01.2 | Please confirm if your appointed responsible named officer also has the responsibility for risk management within your organisation. If not please supply full contact details of the person responsible for risk management |  |
| 1.01.3 | Provide details of the name, contract function and details of any proposed subcontractors you will use |  |
| 1.01.4 | Please provide you overarching policy covering information security/data protection policy. |  |
| 1.01.5 | Are your policies reviewed at regular intervals and if so how often? |  |
| 1.01.6 | In order to assure all security holding and sharing of data CEC require a clear "warranty" from the Supplier that all data provided, stored and accessed at any proposed subcontractor (including Data Centre’s) will be treated with rigour as required by the contract |  |
| 1.01.7 | Please outline how you will monitor and gain assurance that subcontractors are compliant with the security requirements in accordance with the contract terms |  |
| **1.02** | **Confidentiality** |  |
| 1.02.1 | Please confirm how this is provided and managed and/or your agreement to implementing this requirement. |  |
| 1.02.2 | Do you require your staff and subcontractors to confirm confidentiality as part of their conditions of employment? |  |
| 1.02.3 | Provide agreement here that, where at the written request of the Authority, the Supplier shall obtain individual confidentiality statements from supplier’s personnel including subcontractors. |  |
| 1.02.4 | Any passwords stored by the solution should be stored in a manner that prevents them from being read, disclosed or otherwise compromised.  Please describe how the solution meets requirements |  |
| 1.02.5 | The solution’s appointed security supervisors / administrators should be able to issue new passwords in the event of users forgetting their passwords. Users should be prompted to change their password at regular intervals.  Please describe how the solution meets requirements. |  |
| 1.02.6 | The solution shall have full audit trail functionality available and attributable to individual solution users, using role based access permissions. These may include but not be limited to: • Successful login / logout • Unsuccessful login / logout • Unauthorised access (where applicable) • Record or data access attempts • Privileged system changes (e.g. account management, policy changes, device configuration) •Location of access (IP address)  Please describe how the solution meets requirements. Can the log data be exported and in what format should the client wish to import into an internal SIEM (security incident and event management) solution? |  |
| 1.02.7 | The solution shall enable only Authorised Council staff to authorise setup and amend user accounts.  Please describe how the solution meets requirements. |  |
| 1.02.8 | The solution should achieve equivalent strength & configurability of password management as that provided by the Council's implementation of Active Directory, including control over minimum password length, password composition and complexity, frequency of password changes and re-use of passwords.  Please describe how the solution meets requirements.  Please ensure, as a minimum, that your response meets with Council’s Code of Practice:  • A password should be at least eight characters in length.  • Contain characters from three of the four categories: uppercase; lowercase; 0 through 9; or special characters (\*&^%$£”! etc.).  • Not contain two of the same characters consecutively.  • Be difficult for anyone else to guess.  • Be kept confidential and not shared with anyone, not written down, and not included as part of an automated routine e.g. stored in a macro.  • Be changed regularly and not used again for at least 12 months. |  |
| 1.02.9 | Identity management such as SAML, ADFS, Open ID or 2 factor authentication is important in reducing the risk of unauthorised access. Please provide details of any identity management controls that your solution employs.  If SAML is supported, please provide further clarification on what is provided within the SAML token.  Please describe how the solution meets requirements. |  |
| 1.02.10 | Describe how the solution can utilise Identity Management to provide authentication to citizens.  Please describe how the solution meets requirements. |  |
| 1.02.11 | The solution shall provide a mechanism to restrict access to the system, based on user role so that only known endpoints have the ability to connect.  Please describe how the solution meets requirements. |  |
| 1.02.12 | Do you have controls in place to restrict and monitor the installation of unauthorised software onto systems which may host or connect to council data? |  |
| 1.02.13 | Please detail any controls that are in place to segregate client data e.g. when traversing across organisational boundaries over the internet. |  |
| 1.02.14 | Please list how you segregate production data from other non production environments e.g. Development, Test, UAT? |  |
| 1.02.15 | Please describe any controls in place to prevent data leakage or intentional/accidental compromise between tenants in a multi-tenant environment? |  |
| 1.02.16 | Do you restrict, log and monitor access to your information security management systems? (E.g. hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.) |  |
| 1.02.17 | Higher levels of assurance are required on hosted environments to detect potentially suspicious network behaviours and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.  Please list controls for collection, protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory, or regulatory compliance obligations and providing unique user access accountability including voice/call recording.  Responses should also include details of whether :-  File integrity (host) and network intrusion detection (IDS) tools are implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?  Physical and logical user access to audit logs are restricted to authorised personnel?  Audit logs are centrally stored and retained?  Audit logs are reviewed on a regular basis for security events (e.g. with automated tools)?  You use a synchronised time-service protocol (e.g. NTP) to ensure all systems have a common time reference?  Security Information and Event Management (SIEM) is in use and if it merges data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting? |  |
| 1.02.18 | Please list controls that ensure that data is separated appropriately for environments that are used for purposes other than production e.g. test, UAT. Controls should include anonymisation, auditing, access restrictions, logically and physically segregated reduction and non-production environments, and separate retention capabilities. |  |
| 1.02.19 | Have you tested your security incident response plans in the last year? |  |
| 1.02.20 | Please describe the Incident Management measures you will operate within your organisation and how you will implement them – Please attach any relevant policies |  |
| 1.02.21 | Please confirm that you will notify the Authority immediately should any incident occur which could compromise Authority Data |  |
| 1.02.22 | Do third-party agreements include provision for the security and protection of information and assets? |  |
| 1.02.23 | The supplier shall provide assurances on the physical destruction of media containing personal data to prevent accidental disclosure. This may arise due to hardware replacement programme or in the case of contract termination etc.  Employs "Data Destruction Software" certified to recognised international standards, including but not limited to, CESG HMG Infosec Standard No: 5 Secure Sanitisation (Baseline and Enhanced), Navy Staff Office Publication (NAVSO P-5239-26), US National Security Agency Overwrite standard and US Department of Defence Standard, dependant on impact level.  Please describe how the solution meets requirements. |  |
| 1.02.24 | Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alternation, or destruction.  Please confirm audit controls and procedures that are in place across application interfaces or any relevant standards in use in the organisation? |  |
| 1.02.25 | Any access given to 3rd parties must only be to a level for the tasks they are required to perform and must be controlled and logged throughout.  Please describe how the solution meets requirements. |  |
| 1.02.26 | The solution should comply with the principles of the of the UK Data Protection Act 2018.  Please describe how the solution meets requirements and provide details of your compliance including your data registration number. |  |
| 1.02.27 | Please confirm if your organisation is considering off shoring in relation to the proposed solution and that Authority approval will be sought and gained before off shoring processes or storage of Authority Data. |  |
| 1.02.28 | Please confirm whether the implementation of your solution requires any integration with corporate architecture to enable successful delivery.  Please describe the necessary elements needed to facilitate the integration and any resource requirements, including if Browser Extension(s) are used within your solution offering or API including standards adhered to e.g. <https://www.gov.uk/guidance/gds-api-technical-and-data-standards> |  |
| 1.02.29 | Please confirm whether the solution will need to send email from a Cheshire East managed email domain e.g. cheshireeast.gov.uk. If so:  Please provide the IP address of the mail server(s) that will be used so that these can be added as an authorised email server for our domain.  Please confirm that the solution supports DKIM signing of all emails generated. |  |
| 1.02.30 | How do you transfer Authority data to and from your subcontractors? |  |
| 1.02.31 | Please describe how your organisation classifies data and how assets are managed.  Provide any policies for handling, storing, copying or transferring assets i.e. asset registers. |  |
| 1.02.32 | Please confirm if the environment is capable of holding Credit Card data and have relevant PCI compliance (PA DSS, PCI DSS). Please provide further details. |  |
| **1.03** | **Integrity** |  |
| 1.03.1 | Independent reviews and assessments shall be performed at least annually to ensure that the organisation addresses nonconformities of established policies, standards, procedures, and compliance obligations. Please describe how your solution meets this requirement and consider the following :-  -Do you conduct network and application penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?  -Do you have external third party services conduct vulnerability scans and periodic penetration tests to validate risks on your applications and networks?  -Are the results of the penetration tests available to tenants at their request?  -Do you allow tenants to view your ISO 27001 or similar third-party audit or certification reports?  -Do you conduct internal and external audits regularly as prescribed by industry best practices and guidance?  -Are the results of internal and external audits available to tenants at their request?  -Do you permit tenants to perform independent vulnerability assessments? |  |
| 1.03.2 | The solution shall have robust mechanisms for protection against attacks affecting system integrity, availability and confidentiality. The solution’s functional security claims shall be formally and independently accredited.   Please describe how the solution meets requirements and supply evidence of the independent accreditation |  |
| 1.03.3 | Robust controls or counter measures should be provided by the system to ensure the confidentiality, integrity and availability of system data.  Please provide details of any previous data loss, data breach processes and associated policies and incident management processes |  |
| 1.03.4 | What will you do when a vulnerability impacting your product/service is discovered?   * Is there governance and process in place to deal with security incidents (i.e. how are vulnerabilities reported and triaged)? * When vulnerability is discovered, have you thought about the processes which are needed to respond? * Is the product or service maintainable when a security vulnerability is uncovered? For example can the patching process be made easier for the customer? |  |
| 1.03.5 | The solution shall provide end to end encryption which includes data transmitted between client and services i.e. server and back-end platforms (including any login credentials).  Please describe how the solution meets requirements. |  |
| 1.03.6 | Are routine electronic transfers of data containing sensitive data done through secure methods, and is the data encrypted before transfer? |  |
| 1.03.7 | Are encryption methods that meet Advanced Encryption Standards (AES) always used to move sensitive data? |  |
| 1.03.8 | Are ancillary or working data sets containing sensitive data encrypted when not in use? |  |
| 1.03.9 | Organisational policies, industry or government regulations and compliance, may require the use of encryption “**at rest**” to protect corporate data. Please describe if your solution has the option for encrypting “**data at rest**” as part of the proposed solution and what protective marking level the solution is accredited too. |  |
| 1.03.10 | Please confirm details of data segregation which is applied to the tenant data environment to enable controls can be applied (i.e. Retention schedules, deletion policies). |  |
| 1.03.11 | Are scripts accessible and in use to delete or anonymise test data? |  |
| 1.03.12 | Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings? |  |
| 1.03.13 | Are systems in place to monitor for privacy breaches and notify clients expeditiously if a privacy event may have impacted their data? |  |
| 1.03.14 | Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and client data from portable and mobile devices within your organisation, including supply chain 3rd parties (e.g., laptops, cell phones and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organisation’s facilities)? |  |
| 1.03.15 | Please detail any controls around access to client data (including metadata).  Your answer should include :-  Who can request access to data and how this is provide along with any information gathering or collection that takes place including mining of data or metadata.  If you collect or create metadata about client data usage through inspection technologies (search engines, etc.)? |  |
| **1.04** | **Availability** |  |
| 1.04.1 | The solution’s underlying hardware, operating system and software component platforms (i.e. Windows, SQL) must have their own current vendor security patches and firmware updates are applied without causing disruption to the solution and without voiding the systems support arrangements.   Please give examples of where critical security vulnerability has been identified in the past and state timeline for issuing a tested patch. |  |
| 1.04.2 | Suppliers shall detail the controls in place to ensure their systems are patched efficiently and effectively and cover against potential threats (this can include zero day exploits and known threats). |  |
| 1.04.3 | The supplier shall detail how the solution shall enable the installation of software updates without requiring the solution to be re-installed and without causing major operational disruption. |  |
| 1.04.4 | Can you confirm that any external facing URL is sufficient for the data classification held and free from known vulnerabilities? The Council will use “Web Check" offered by the NCSC (National Cyber Security Centre), as part of its audit check on an annual basis to confirm assurance to minimal standards. The use of Web Check is to validate user data is protected, if protective technologies such as HTTP strict transport security (HSTS) and content security policy (CSP) are in place. |  |
| **1.05** | **Compliancy & Certification** |  |
| 1.05.1 | The system/supplier should comply with industry recognised standards and guidance, such as:  • ISO 20000 (ITIL)  • ISO 25777 (ICT Continuity). • ISO 25999 (Business Continuity). • ISO 9001:2000. • ISO 27001 (Information Security Management System) (formerly BS 7799). • ISO 270035:2011 (Information Security Incident Management) • ISO 14001 (Environmental Management System)  Please provide details of any security certification that your company holds  Please describe how the solution meets requirements |  |
| 1.05.2 | Please describe how the system complies with all current relevant legislation pertaining to computer systems and data management. This will include specifically, although not exclusively, the Computer Misuse Act and the Data Protection Act. Also describe how this compliance is reviewed and maintained.  Please describe how the solution meets requirements |  |
| 1.05.3 | Please detail whether you have been assessed and awarded certification to the standards set out within the UK Governments “Cyber Essentials or Cyber Essentials Plus Scheme”, including any supporting evidence. |  |
| 1.05.4 | Please detail your awareness and adoption of the responsibilities set out in the [EU Directive 2016/2102](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L2102) due for adoption September 2018, by the UK Government.  Further guidance is included below:  <https://ec.europa.eu/digital-single-market/en/web-accessibility>  <https://webdevlaw.uk/2016/12/05/plain-english-guide-eu-accessibility-directive/> |  |
| 1.05.5 | Please detail your awareness and adoption of the responsibilities set out in the EU Directive for [NIS (Network and Information Systems)](https://www.ncsc.gov.uk/guidance/introduction-nis-directive) and [Directive 95/46/EC GDPR (General Data Protection Regulation)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679) due for adopted May 2018, by the UK Government.  Further NCSC (National Cyber Security Centre) guidance is included below:  <https://www.ncsc.gov.uk/guidance/nis-guidance-collection>  <https://www.ncsc.gov.uk/guidance/cyber-assessment-framework-caf> |  |
| 1.05.6 | If this system requires or would benefit from an Address Validation/Lookup feature then please note that Cheshire East Council’s preferred methodology is that the system interfaces to an in-house web-service (details of which are available on request) which provides access to our centralised Address repository (and which is maintained daily). This ensures that any Address Data accessed is always the most current version available.  In the event that the system is not capable of using the CE web-service, then National Land and Property Gazetteer (NLPG) data can be provided at a regular frequency via Change Only Update (COU) files in their native format (currently DTF 7.3.3.1)  Please be aware that any supplier who wishes to access Cheshire East Council’s LLPG/NLPG data (in whatever guise) will be expected to sign the PSMA (Public Sector Mapping Agreement) Contractor licence which is available here  <https://www.ordnancesurvey.co.uk/docs/licences/psma-standard-contractor-licence-form-field.docx>  Prospective suppliers must confirm   1. whether they propose to utilise Cheshire East Council’s LLPG/NLPG data.   If the answer to (i) above is affirmative, prospective suppliers must then also confirm   1. the proposed method by which their system will access the data (web-service or consumption of raw data into an internal Gazetteer (Address lookup database)) 2. acceptance of the terms found in the PSMA Contractor Licence 3. the coverage of the data required (Cheshire East Council or Cheshire East Council plus neighbouring Authorities) 4. whether the Unique Property Reference Number (UPRN) associated with an address is stored within the system. Please note that Cheshire East Council interprets the UPRN as Personally Identifiable Information (PII) under GDPR. |  |
| **1.06** | **Hosted Solution** |  |
| 1.06.1 | Please confirm if data will be hosted and processed within the EEA (European Economic Area) and adherence to Chapter 5 (Transfers of personal data to third countries or international organisations) of GDPR (General Data Protection Regulation) in relation to data transfers.  Please review the[*ICO Guidance*](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/)on data transfers and provide details of data centre locations and service management location. |  |
| 1.06.2 | The authority requires provision for data protection and the archiving and deletion of personal data. The supplier must provide details showing how these requirements will be met. |  |
| 1.06.3 | Please detail how the solution is presented to users (i.e. over the internet, Corporate Client / Server install, Private VPN connection). |  |
| 1.06.4 | Has a technical analysis of the design and/or implementation been conducted from a security point of view?  - A review could cover all or a part of the development lifecycle, from Concept through to Design, Implementation and Operation  - An analysis can be done using internal personnel with cyber security expertise, or use of an independent third party organisation  - Consider what a reviewer might need in terms of documentation, source code or physical access to the product/service |  |
| 1.06.5 | Do you know what third party elements your product is dependent on, and do you have adequate support when vulnerabilities are found in them? |  |
| 1.06.6 | Please detail how the solution will be hosted (e.g. Public Cloud, Private Cloud) and whether it will be delivered as SAAS, PAAS or IAAS. Include in the response responsibility for the following (e.g. tenant, hosting provider, suppler).  *Data Security  Application Security  Platform Security  Infrastructure Security  Physical Security*  Please confirm awareness and adoption of NCSC Cloud Security Principles <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>  <https://www.ncsc.gov.uk/design-principles> |  |
| **1.07** | **Network compatibility** |  |
| 1.07.1 | Is the solution capable of traversing a network that uses Network Address Translation (NAT)?  Please describe how the solution meets requirements. |  |
| 1.07.2 | List all of the TCP ports that the system uses in all communications across the network. |  |
| 1.07.3 | What network protocols are to be used? e.g. DNS, DHCP, TCP, TFTP, HTTP, HTTPS, UDP etc. Please provide details. |  |
| **1.08** | **Business Continuity and Disaster Recovery (BCDR)** |  |
| 1.08.1 | The supplier is to provide details of their disaster recovery/business continuity (BCDR). Please provide a method statement demonstrating how it proposes to manage operational risks and what steps it will put in place to ensure that the likelihood of a disaster occurring is reduced/mitigated. |  |
| 1.08.2 | Please provide details of protective monitoring undertaken within the service platforms.  How many premises/sites will be used in the delivery of this solution? |  |
| 1.08.3 | If multiple sites are involved in the delivery of the solution then please describe your premises setup. E.g. whether it involves being a sole occupier of buildings owned by your organisation or within a multiple occupancy site that your organisation does not own, or another configuration. |  |
| 1.08.4 | Please describe the building security physical and technical measures you will operate for your premises to ensure that Authority Data is protected from unauthorised access, theft or damage – Please attach any relevant policies. |  |

|  |  |  |
| --- | --- | --- |
| **1.09** | **Legal and Contractual Obligations** |  |

|  |  |  |
| --- | --- | --- |
| 1.09.1 | Describe the specific measures you will operate and how you will implement them - please attach the relevant policies  Describe organisational and individual responsibilities for information security and explain how they are clearly defined. Are all staff aware of the security breach policy and potential sanctions available for inappropriate behaviour?  Is a process in place to ensure your organisation is kept up to date with relevant current and emerging best practice? |  |
| **1.10** | **Personnel Security** |  |

|  |  |  |
| --- | --- | --- |
| 1.10.1 | Please provide details of personnel security screening to manage the security vetting of staff |  |
| 1.10.2 | How many of your personnel access, handle and process Authority Data? |  |
| 1.10.3 | How many of your subcontractor personnel access, handle and process Authority Data? |  |
| 1.10.4 | Please provide details of what and how audit records are provided to the client to monitor access to the service or data held. |  |

|  |  |  |
| --- | --- | --- |
| **1.11** | **Staff Training and Awareness** |  |

|  |  |  |
| --- | --- | --- |
| 1.11.2 | Please describe the specific measures you operate and there implementation - please attach the relevant policies – if using Social Media.  Is your organisation proposing to use any form of social media in the delivery of this service? If yes, please provide detail? Please confirm that you will not use any form of social media, without prior approval/consent by Cheshire East Council. |  |