**Cheshire East Council ICT Security – (Private Cloud)**

**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** | **Confidentiality** | **Response** |
| 1.01.1 | 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. |  |
| 1.01.2 | 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. |  |
| 1.01.3 | 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? |  |
| 1.01.4 | The solution shall enable only approved Council staff to authorise setup and amend user accounts.  Please describe how the solution meets requirements. |  |
| 1.01.5 | 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. |  |
| 1.01.6 | 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.  Do you provide clients with strong (multifactor) authentication options (digital certs, tokens, biometrics, geographic location? etc.) as an authentication factor for user access?  Please describe how the solution meets requirements. |  |
| 1.01.7 | Describe how the solution can utilise Identity Management to provide authentication to citizens, if required.  Please describe how the solution meets requirements. |  |
| 1.01.8 | Please list how you segregate production data from other non-production environments e.g. Development, Test, UAT? |  |
| 1.01.9 | 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. |  |
| 1.01.10 | 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. |  |
| 1.01.11 | 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? |  |
| 1.01.12 | The solution should comply with the principles of the of the UK data protection act 1998.  Please describe how the solution meets requirements and provide details of your compliance. |  |
| 1.01.13 | Please confirm whether the implementation of your solution requires any integration with corporate architecture to enable successful delivery e.g. email.  Please describe the necessary elements needed to facilitate the integration and any resource requirements. |  |
| 1.01.14 | Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards and adhere to applicable legal, statutory, or regulatory compliance obligations.  Please list the controls that you have in place for example:- Do you publish a list of all APIs available in the service and indicate which are standard and which are customised? Automated source code analysis tool to detect security defects in code prior to production? Manual source-code analysis to detect security defects in code prior to production? Assurance that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security? Review of applications for security vulnerabilities and address any issues prior to deployment to production? |  |
| 1.01.15 | 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. |  |
| 1.01.16 | Are controls in place to prevent unauthorised access to your application, program or object source code, and assure it is restricted to authorised personnel only? |  |
| **1.02** | **Integrity** |  |
| 1.02.1 | 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 :-  - Network and application penetration tests of the service infrastructure regularly, as prescribed by industry best practices and guidance?  -External third party services employed to conduct vulnerability scans and periodic penetration tests to validate risks on your applications?  -Do you allow clients 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 clients at their request?  -Do you permit clients to perform independent vulnerability assessments? |  |
| 1.02.2 | 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. |  |
| 1.02.3 | Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data? |  |
| 1.02.4 | The solution shall provide end to end encryption which includes data transmitted between clients and services i.e. server and back-end platforms (including any login credentials).  Please describe how the solution meets requirements. |  |
| 1.02.5 | Are routine electronic transfers of data containing sensitive data done through secure methods, and is the data encrypted before transfer? |  |
| 1.02.6 | Are encryption methods that meet Advanced Encryption Standards (AES) always used to move sensitive data? |  |
| 1.02.7 | Are ancillary or working data sets containing sensitive data encrypted when not in use? |  |
| 1.02.8 | 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 capability for encrypting “**data at rest**” as part of the proposed solution and what protective marking level the solution is accredited too. |  |
| 1.01.9 | Please list the change controls process for development of new or updated applications, systems, databases, infrastructure, services, operations and facilities?  Indicate whether you follow specified standards e.g. ITIL |  |
| 1.01.10 | Do you have controls in place to ensure that standards of quality are being met for all software development? |  |
| 1.01.11 | Is documentation describing known issues with certain products/services available? |  |
| 1.01.12 | Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings? |  |
| 1.01.13 | Are systems in place to monitor for privacy breaches and notify clients expeditiously if a privacy event may have impacted their data? |  |
| 1.01.14 | 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)? |  |
| 1.01.15 | Do you provide clients with a role definition document clarifying your administrative responsibilities versus those of the client? |  |
| 1.01.16 | 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.)? |  |
| **1.03** | **Availability** |  |
| 1.03.1 | Suppliers shall detail the controls in place to ensure their systems and solutions are patched efficiently and effectively and cover against potential threats (this can include zero day exploits and known threats). |  |
| 1.03.2 | 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** | **Compliancy & Certification** |  |
| 1.04.1 | 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 |  |
| 1.04.2 | 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 |  |
| 1.04.3 | 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** | **Hosted Solution** |  |
| 1.05.1 | 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. |  |
| 1.05.2 | 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. |  |
| 1.05.3 | Please detail how the solution will be hosted (e.g. Private Cloud) and responsibility for the following:  *Data Security  Application Security  Platform Security  Infrastructure Security  Physical Security*  Please confirm awareness and adoption of CESG Cloud Security Principles <https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles> |  |
| **1.06** | **Network compatibility** |  |
| 1.06.1 | Is the solution capable of traversing a network that uses Network Address Translation (NAT)?  Please describe how the solution meets requirements. |  |
| 1.06.2 | List all of the TCP ports that the system uses in all communications across the network. |  |
| 1.06.3 | What network protocols are to be used? e.g. DNS, DHCP, TCP, TFTP, HTTP, HTTPS, UDP etc. Please provide details. |  |
| **1.07** | **Business Continuity and Disaster Recovery (BCDR)** |  |
| 1.07.1 | 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. |  |

|  |  |  |
| --- | --- | --- |
| 1.07.2 | Please provide details of personnel security screening and security education undertaken by employees. |  |
| 1.07.3 | Please provide details of what and how audit records are provided to the client to monitor access to the service or data held. |  |
| 1.07.4 | Please provide details of protective monitoring undertaken within the service platforms. |  |
| 1.07.5 | Do you provide tenants with documentation showing the transport route of their data between your systems? |  |

|  |  |  |
| --- | --- | --- |
| **1.07** | **Network Requirements** |  |

|  |  |  |
| --- | --- | --- |
| 1.07.1 | What is the maximum required bandwidth for a single connection to the system (one user)? Is this scalable equally to greater numbers?  e.g. 1 client = 1meg so 10 clients = 10meg  Please describe how the solution meets requirements. |  |
| 1.07.2 | What is the peak bytes/second transmitted to the network by the heaviest using client? |  |
| 1.07.3 | What is the maximum permissible network latency between Client and Server in milliseconds? |  |
| 1.07.4 | What is the average bytes/second transmitted to the network by the heaviest using client? |  |
| 1.07.5 | What is the peak bytes/second transmitted to the network by the system under its maximum load? |  |
| 1.07.6 | What is the average bytes/second transmitted to the network by the system under its maximum load? |  |
| 1.08.1 | Does the application require a link through the wide area network to an external network (e.g. the Internet)? What Internet sites and protocols does the application need to contact? |  |

|  |  |  |
| --- | --- | --- |
| **1.09** | **Remote support requirements** |  |

|  |  |  |
| --- | --- | --- |
| 1.09.1 | Does the supplier of the system require any remote support connections into the wide area network for ongoing support or upgrades by the supplier?    Please describe the requirements. |  |