**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** | **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 Authorised 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.Please describe how the solution meets requirements. |  |
| 1.01.7 | Describe how the solution can utilise Identity Management to provide authentication to citizens.Please describe how the solution meets requirements. |  |
| 1.01.8 | 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. |  |
| 1.01.9 | 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. |  |
| 1.01.10 | 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. |  |
| 1.01.11 | 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. |  |
| 1.01.12 | 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. |  |
| 1.01.13 | 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. |  |
| **1.02** | **Integrity** |  |
| 1.02.1 | 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 |  |
| 1.02.2 | 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 and associated policies and incident management processes |  |
| 1.02.3 | 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. |  |
| 1.02.4 | Are routine electronic transfers of data containing sensitive data done through secure methods, and is the data encrypted before transfer?  |  |
| 1.02.5 | Are encryption methods that meet Advanced Encryption Standards (AES) always used to move sensitive data?  |  |
| 1.02.6 | Are ancillary or working data sets containing sensitive data encrypted when not in use? |  |
| 1.02.7 | 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.  |  |
| 1.02.8 | 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).  |  |
| 1.02.9 | Are scripts accessible and in use to delete or anonymise test data? |  |
| **1.03** | **Availability** |  |
| 1.03.1 | 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. |  |
| 1.03.2 | 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). |  |
| 1.03.3 | 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. |  |
| 1.03.4 | 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.  |  |
| **1.04** | **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 holdsPlease 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 Information Commissioners Office states that data should only be hosted and processed within the EEA or a country considered safe by the ICO. The supplier should confirm that data will be hosted and processed within the EEA. Please provide details of data centre locations and the service management location. |  |
| 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 is presented to users (i.e. over the internet, Corporate Client / Server install, Private VPN connection). |  |
| 1.05.4 | 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 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. |  |