Attendance Monitoring Service & ePEP for LACs
IT Procurement Technical Requirements

Table of Contents

1 Standards & Legal Requirements 2
2 Security 2
3 Client Access 3
4 Hosted/Cloud Services 3
5 Business Continuity 4
6 Systems Integration 4
7 Reporting 5
8 Data Migration 5

1 Standards & Legal Requirements

Ref	Requirement
1.1	Suppliers must have ISO 27001 or Cyber Essentials Plus accreditation. Suppliers must state which and provide evidence to support it.
1.2	Where the system, in part or as a whole, is accessed via a web browser or mobile application the system must comply with the Public Sector Bodies (Website and Mobile Applications)(No. 2) Accessibility Regulations 2018. This should comply with the latest approved specification of the W3C Web Content Accessibility Guidelines, e.g. WCAG 2.2 AA accessibility standard. Understanding accessibility requirements for public sector bodies - GOV.UK (www.gov.uk)
1.3	The supplier must confirm, and demonstrate how, their system complies with the General Data Protection Regulations (UK-GDPR).
1.4	Where the system, in part or as a whole, is accessed via a web browser the system must comply with the GDPR/PECR legislation regarding cookie management.

2 Security

Ref	Requirement
2.1	The system must support single sign-on and be compatible with the Azure AD Identity Provider. The supplier must demonstrate how it will support this requirement using either SAML, OpenIDConnect, OAuth2 or WSFed.
2.2	The system maps its authorisation model from Azure Active Directory groups and/or roles with an automated exchange of user information using either SCIM, MSGraphAPI or is Claims-Aware
2.3	Where access is supported via standalone username & password, usernames must be unique, and password complexity must be configurable to meet guidance issued by the National Cyber Security Centre (NCSC). Suppliers must provide details on the configuration options for both usernames and passwords, including: • Minimum and maximum length. • Password complexity. • Validity period for passwords.
2.4	Systems using standalone username & password should support the use of Multi Factor Authentication.
2.5	The system should provide a means by which we can provision, edit, suspend and de-provision user accounts without requiring input from the system supplier.
2.6	Where standalone usernames & passwords are used, the system must lock out a user account after a configurable number of failed login attempts.
2.7	Where standalone usernames & passwords are used, passwords must be suitably salted and hashed. Passwords must never be stored or displayed as clear text.
2.8	Where standalone usernames & passwords are used, the system must provide a secure means by which users can reset their password without intervention by our staff or the system supplier.
2.9	Where standalone usernames & passwords are used, users must be prompted to change their password the next time they access the system after their password has been changed by a system administrator or the password validity period has expired.
2.10	The system must be able to restrict access and functionality based on user role, and user roles must be configurable in the system.
2.11	The system should automatically log users out of the system after a configurable amount of time of inactivity. System and database integrity must be maintained when this happens.
2.12	The system must provide a full audit trail of user activity, unless it is a public facing website.
2.13	The system must encrypt data in transit, both within the corporate network and across public networks. The supplier must state how this is achieved, the type and strength of encryption used, and who holds the encryption keys.
2.14	The system should encrypt sensitive data at rest. The supplier must state how this is achieved, the type and strength of encryption used, and who holds the encryption keys.

Ref	Requirement
2.15	The supplier must allow third party specialist testing of the system (accessibility, security, penetration testing, etc.) where deemed necessary by the council.
2.16	The supplier must state how their system: • Supports multi-tenancy, where two or more organisations use the one system. • Identifies what data belongs to which organisation. • Controls access to one or more organisations' data; some users in shared service roles may need to work across more than one organisation. In this scenario the users should not require multiple logins.

3 Client Access

Ref	Requirement
3.1	Suppliers must describe how the system is accessed, be it via a thick client application, a mobile device application, and/or a web browser. This may differ depending on the part of the system being accessed. The preference is for a web browser-based system for PC users, and mobile apps on smartphones & tablets.
3.2	Where the system, in part or as a whole, is accessed via a web browser the system must work in the latest current version and current version minus 1 of the following web browsers, both desktop and mobile versions: • Google Chrome • Mozilla Firefox • Apple Safari • Microsoft Edge Chromium (organisation default)
3.3	Where the system, in part or as a whole, is accessed via a web browser, cookies should only be used with sensible expiry dates consistent with the shelf life and usefulness of the data. Where relevant, public users, should be able to make an informed choice about the cookies that are used when using the system.
3.4	The system must be fully responsive and adapt to different screen sizes, input methods (keyboard & mouse, touch enabled interface, etc.) appropriate to desktop, tablet, and smartphone devices. Suppliers need to state any limitations the system has.
3.5	Where a thick client is used, the supplier must provide the means and support to deploy the thick client and any prerequisites via Microsoft Endpoint Manager (formally Intune) In the event of a legacy deployment, Microsoft System Centre 2019 Configuration Manager application install routine for the ease of deployment.

4 Hosted/Cloud Services

Ref	Requirement
4.1	If the proposed system is a cloud solution, all servers and data must always be contained within UK only datacentres.
4.2	The supplier must provide details of the service availability SLA and where any SLA is missed the supplier must provide a proportional service credit.
4.3	The supplier is required to provide details of the disaster recovery and business continuity plans in place for the system, including recovery time objectives and recovery point objectives.
4.4	The supplier must demonstrate the security (both physical and IT related) in place for the hosting environment, including details on how client access to the system is secured.
4.5	Where the supplier uses datacentres provided by a third-party they must provide the third parties details.
4.6	The supplier must prove the datacentre(s) in use are approved for UK Government use to the 'Official' Government Security Classification Policy (GSC).

Ref	Requirement
4.7	The supplier must undertake all work relating to applying patches, bug fixes, upgrades, server restarts, etc. that are required to keep the solution operational, up to date, & secure. Work must take place within agreed maintenance windows.
4.8	The supplier is required to list the standard maintenance windows.
4.9	The supplier must state their approach to maintaining the versions of the underlying software (operating system, database software, etc.) to ensure that the system runs on the latest versions when possible.
4.10	The supplier must describe their approach to monitoring, managing, and reporting to the council the following: • Server health monitoring checks. • Operating System checks. • Log file checking. • Patches checked and applied. • Database maintenance. • Test database restore. • Anti-virus updates checked and applied. • Check for malware & intrusion. • Full system availability. • Data connection checks. • Report on maximum bandwidth used. • Report on average bandwidth used.
4.11	The supplier must demonstrate compliance with the NCSC cloud based principles guidance - https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

5 Business Continuity

Ref	Requirement
5.1	The supplier must provide evidence of the regular testing (at least annually) of Business Continuity Plans
5.2	The supplier must provide evidence that their business continuity planning has made provision for incidents of national impact e.g. national power outage, pandemic

6 Systems Integration

Ref	Requirement
6.1	Where the system sends email on behalf of the council, it must be capable of using Exchange Online as the SMTP relay.
6.2	The system must be able to import and export data from multiple line of business systems. The supplier must state how the system will achieve this, what tools the system includes to create & manage the imports & exports, and whether the imports & exports can be created by council staff or if they can only be created & managed by the supplier.
6.3	The supplier must describe any APIs that the system has for exchanging data with other systems.
6.4	The supplier must state any third-party systems they have already integrated their system with.
6.5	The supplier must state what previous experience they have of integrating their system with the following third-party systems: • Liquid Logic (System C) LCS / EYES
6.6	The supplier must provide contact details for other local authorities where the supplier has integrated their system with any applications on the above list.

7 Reporting

Ref	Requirement
7.1	The system should have the ability for users to create reports, report templates, and publish them via the reporting system for other users to consume.
7.2	The system should include the ability to create ad-hoc reports on data held in the system.
7.3	The system should be able to output reports as PDF and Excel files as a minimum.
7.4	The system should allow reports to be created automatically on a scheduled basis.
7.5	The system should present database tables, views, field names, etc. in an intelligible way that users will recognise.
7.6	The supplier must state if reporting is against a snapshot of the data in the system, and if so, how often the snapshot is updated, or against the live database.
7.7	The system should be able to report on the quality of the data it holds.
7.8	The system should be able to produce reports showing lists of records, as well as summary metrics to support performance and management reporting.
7.9	The system should allow calculated fields to be derived from the data in the system and used in reports, e.g. the number of working days between a case being opened and closed, etc.
7.10	The supplier should list any additional reporting features and/or products that are available to users, which would enhance the reporting capability (e.g. reporting OLAP cubes, etc.). Suppliers must state if this forms part of their standard system or as an add-on, together with any limitations (e.g. certain modules which cannot be reported on, etc.).
7.11	The system must state which statutory report templates come with the system.
7.12	The system must allow users to enter parameters when running reports where relevant, e.g. a date range, a number/amount range, text search, etc.
7.13	The system should allow report parameter values to be changed and the report rerun without having to create/define the report again from scratch.
7.14	The system must include the ability to sort and filter report contents.

8 Data Migration

Ref	Requirement
8.1	The supplier must state how they will migrate data from a current line of business system.
8.2	The supplier must state any third-party systems they have already undertaken data migration to their system.
8.3	The supplier must provide contact details for other local authorities where the supplier has undertaken a similar data migration to their system.
8.4	The supplier must provide an outline exit plan, with estimated costs, to cover the work to support the controlled migration of data to an alternative supplier at the end of the contract period. The supplier must include a description of the preferred open data format that will be used.