3- Specification (BTT)

Contract Reference

T00215HBP

Contract Title

Harbour Management System

Contents

1 Specification

1.1 Overall Scope and Nature of the Requirement

Torbay Council has a requirement for a Harbour Management system which will be used to record details of all Harbour Customers, together with details of their vessels and any facilities and services they are paying for, either on a long-term contract (annual) basis or for a short term. This will include Harbour Dues, Mooring Fees, various licences (including Fish Buyers and Sub-Contractors), with scope to extend to other areas, such as Beach Huts, in the future. There are currently approximately nine hundred (900) berths in three (3) Harbours – Torquay, Brixham and Paignton.

The System must meet the Specification as defined in Appendix A. It should embrace modern technology such as the use of mobile devices and visual displays as opposed to fully textual information. An element of Customer Self Service would also be of benefit, although this can be added in a later Release of the software. The Authority has no preference as to whether the system is hosted externally or on the Authority's servers.

The System **should not** store any financial information or generate Invoices (either for annual contracts or ad hoc charges) as this will be handled by our Financial System – Advanced Business Solutions (ABS) e5. We will require substantial integration between the two systems and this is detailed in Appendix B.

The Authority is looking to purchase a non-exclusive Perpetual Licence for the Software. There will be a maximum of nine (9) Harbour users using the system concurrently. However, this number may increase or decrease during the period of Contract.

Torbay Council reserves the right to consider all proposals submitted and to award (or not award at all) upon Contract Award, depending on the most appropriate solution within the Most Economically Advantageous Tender (MEAT) submitted.

Acceptance of the System will be as defined within the Acceptance Procedures and Acceptance Testing, within Schedule Six (6) of the of the attached Software Licence, Maintenance & Hosting Agreement).

1.2 Mandatory Pass/Fail Requirements (Yes/No answers)

1.2.1 The System (specifically the Version being proposed for the Authority), excluding the integration specified in Appendix B, must

- be fully developed and currently in Live use (not Beta Testing) in at least two (2) sites in the European Union.
- meet the System Requirements as defined in Appendix A.
- be capable of integrating with Advanced Business Solutions' E5 Financial Management System as detailed in Appendix B.
- be supplied via a non-exclusive Perpetual Software Licence.

- be supplied with at least one environment in addition to the Live environment, to be used for Testing and Training purposes.
- be kept fully functional with all supported versions of third party components, systems etc, for example, databases, operating systems including mobile devices, report tools, browsers or any other products.
- be covered by a Service Level Agreement (SLA) for providing comprehensive technical support for the System with efficient response and resolution of problems. The SLA needs to cover method(s) of incident reporting, incident categorisation, response times, methods of support (including remote support), out-of-hours support, escalation processes, volume of use restrictions and any occasions where additional costs would be applicable.
- utilise Server software running on either a Windows or Linux operating system.
- have a database which is MS SQL 2008 R2 (or higher) Standard Edition, Oracle Standard Edition (that does not use any oracle features that incur extra licence fees beyond the basic licence) or a product that is freely available for commercial use.
- be capable of supporting Batch interface feeds into and out of the System, to be executed in accordance with agreed timetables.
- contain parameters which can be set to enforce timeouts

1.2.2 Training must be provided to support the implementation of the System.

1.2.3 Data must be migrated from the Authority’s current Harbour Management system (HMS supplied by Harbour Systems) in an accurate, correct and timely manner. As a minimum this data will comprise Customer and Vessel data. Authority resources will be provided to extract data from the existing system.

1.2.4 It must be possible to use Virtual server(s) for the Application and Database.

1.2.5 The Supplier must have technical and procedural security measures in place to prevent:

- Unauthorised or unlawful processing of Personal Data
- Accidental loss or destruction of or damage to Personal Data.

1.2.6 For web functionality the Authority must have full editorial capability over the style of the web pages and the content must fully adopt responsive web design. (**Note that this mandatory requirement only applies if the System contains web functionality)**

1.2.7 For web based Customer Self Service functionality, **(Note that these mandatory requirements only apply if the System contains customer self service web functionality)**

- the Supplier must provide up-to-date documentation from a Penetration test undertaken by a reputable third party security vendor and evidence that any high priority items have been addressed. If this is not immediately available the Supplier must guarantee that this will be in place by the time the Contract is signed.

- the Authority is striving towards maintaining W3C html, CSS and AA accessibility standards. The Supplier must provide assurance that any enforced format or layout requirements imposed by them will meet at least AA standards

1.2.8 For configuration changes or technical support, the Supplier must agree to adhere to the following rules when accessing the System remotely on the Authority's servers:

- The Authority insists on all remote access for support and maintenance being by prior arrangement with nominated Authority employees.
- Authority contacts will provide a one-time pass code for each session. Access is achieved via a suitable remote client (e.g. RDP, SSH) hosted by a public terminal server.
- Data / file transfer must be by prior agreement with Authority contact.
- The Authority requires assurance that all Supplier's technicians requiring Remote Desktop sessions use managed devices (where the configuration is controlled by the Supplier) when connecting to the Authority and the Supplier needs to register the external IP address(s) with our firewall in order to provide remote access.
- Any non-Authority device connecting to the Authority's network must be running up-to-date anti-virus and anti-spyware software and have an active application firewall.

1.3 System Requirements

These are defined in Appendix A and will be evaluated by a Demonstration.

1.4 Integration Requirements

These are defined in Appendix B and will be evaluated by a Method Statement.

1.5 Technical Requirements

1.5.1 The Supplier should provide the following information on how the System will be initially implemented and then supported during the term of the Contract with the Authority (Method Statement):

- a clear overview of each component of the System and how it is licensed (including whether this is per Harbour, per Berth or per User) so the Authority knows exactly what it needs to purchase in order to meet the functionality required. Ideally to include an infrastructure diagram showing how the components are interconnected.
- a high level Implementation plan for the software to be implemented for the Authority, giving an indication of the main processes required and estimates of the time required.
- details of the System "Roadmap", i.e. a plan of future changes and enhancements, which should span at least 12 months in the future.

- details of the Service Level Agreement (SLA) for supplying comprehensive technical support for the System. The SLA needs to cover method(s) of incident reporting, incident categorisation, response times, methods of support (including remote support), out-of-hours support, escalation processes, volume of use restrictions and any occasions where additional costs would be applicable.
- details as to the frequency of changes to the software (Releases/Versions, and patches), who will be installing these changes and also details on the extent to which previous and alternative versions of the System are supported.
- confirmation that Client software application components (if any) provided as part of the solution are capable of unattended install.
- a list of the mobile devices supported by the System.
- a list of the Browsers (and versions) that are supported by the web functionality (if any) in the System.
- confirmation that System documentation is provided – as a minimum, this should be a User Manual and a database schema, in hard copy or electronic format.

1.5.2 The Supplier should provide the following information on the security measures which have been adopted when designing, developing, implementing and supporting the system (Method Statement):

a. details of the system’s password policy, which should incorporate encryption, use of mixed case, numbers and special characters, minimum length, expiry, limit on login attempts, logging of unsuccessful login attempts and “forgotten password” functionality.

b. confirmation that any system or scripted passwords can be changed from their default settings within the System. (Will include where application processes need access rights to other components to execute or interface with.)

c. details of the system’s integration with corporate security and authentication systems, for example Active Directory, so that Authority Users do not have to log into the system separately from their main workstation login.

d. details of the system’s User registration process for the Authority’s customers or links with any third party solutions to provide this functionality. Also, details of any API’s to allow the Authority’s portal to drive self service registration and authentication (for example, the use of SAML tokens).

e. details of the technical and procedural security measures in place to prevent:

   - Unauthorised or unlawful processing of Personal Data
   - Accidental loss or destruction of or damage to Personal Data.

f. up-to-date documentation from a Penetration test undertaken by a reputable third party security vendor and evidence that any high priority items have been addressed, if the application contains any web based Customer Self service functionality.

1.6 Minimum Mandatory Requirements for Hosted Solutions

1.6.1 The Authority must

- have free (of additional charge) access to its data for raw extraction. This can be supplied by any of the following: (1) By the Supplier providing full read access (not limited to standard working hours) to the Authority's dataset for a limited number of individuals within the Authority; or (2) Local replication or (3) Remote replication to the Authority’s site.
- be supplied with all of its production data (in a format and time to be specified), with an appropriate database schema, at the end of the Contract Period.
- be able to create new interface feeds/data extraction processes to run on the hosted system. This includes creating the gateways to allow data to be placed for collection and or directly accessed (via web interface in real time).

1.6.2 The Supplier must

- have a Service Level Agreement (SLA) for the hosting of the System. As a minimum the SLA needs to cover ‘Back-Ups’, System Restore, Integration with other Systems, System Availability/Reliability, Service Credits, Turnaround Time within four (4) working days for Live to Test or Training Environment refreshes, Turnaround time within two (2) working days of changes in access rights to data or services, loading of Patches and Upgrades (including Patches and Upgrades to Operating Systems and Third Party Components) regardless of the environment, Reaction to information on potential security breaches and Provision of Data at end of Contract period.
- have general security procedures in place. These must include adherence to recognised standards, for example ISO/IEC 27001 (proof of compliance to be made available upon request). Also, audits by a reputable third party (details of audits to be made available upon request).
- take measures to ensure that only the Authority and approved personnel can access its own dataset.
- ensure that the Authority’s data will not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
- have robust Business Continuity procedures in place such that they can guarantee maximum down time of no more than 48 hours in the event of a major incident (e.g. a flood or fire that results in the loss of computers, telephones, premises etc.)

1.6.3 The solution must

- provide an availability level of 99.5% measured over a calendar month: twenty four hours a day/seven days a week (24* 7).

- facilitate automatic recovery of application files following a system break and the ability to automatically re-update files to the point of the break without the necessity for manual re-keying of data by the users.
- ensure that all data is encrypted in transit.
- contain a mechanism for holding data messages (and making a speedy recovery) in the case of systems, connections or other components being out of action preventing normal data flow from one site to the other.

1.7 Contract and Performance Review Requirements

1.7.1 The Supplier must

- Have a named contract manager.
- Conduct regular contract review meeting, periods will be agreed post contract award.
- In support of the meetings, we would require management meeting reports, the structure and format will be agreed with the contract awards.