Report author: Ian Milner
Tel: 07891275470

Leeds CITY COUNCIL

Report of: Service Development - Security

Report to: Chief Digital and Information Officer

Date: 1st July 2018

Subject: Report to seek approval to waive contract procedure rule 8.1 & 8.2 entering into a contract for an Enterprise Agreement for Entrust SSL Certificate Renewal.

Are specific electoral Wards affected? If relevant, name(s) of Ward(s):	☐ Yes	☒ No
Are there implications for equality and diversity and cohesion and integration?	☐ Yes	☒ No
Is the decision eligible for Call-In?	☐ Yes	☒ No
Does the report contain confidential or exempt information? If relevant, Access to Information Procedure Rule number: Appendix number:	☐ Yes	☒ No

1. Summary of main issues

1.1. Leeds City Council use Secure Sockets Layer (SSL) Certificates * to encrypt and secure HTTPS public facing services.

1.2. The current support and maintenance contract expires 11th September 2018. A new contract is required to allow the council to publish secured web content.

2. Recommendations.

2.1. The Chief Digital and Information Officer is recommended to approve the waiver of contract procedure rule 8.1 and 8.2 entering into a contract with Entrust Limited for the provision of an Enterprise Account to support and maintain the councils SSL Certificates for a period of 3 years at a total cost of £11,535.36.

* SSL stands for Secure Sockets Layer. It provides a secure connection between internet browsers and websites, allowing you to transmit private data online. Sites secured with SSL display a padlock in the browsers URL and possibly a green address bar if secured by an EV Certificate. Reference https://www.instantssl.com/ssl.html

Purpose of this report.

1. Background information.

1.1. The council uses SSL Certificates to enable secure communications for external web services.

1.2. The council currently use Entrust Limited to manage SSL. Entrust provide a management suite and the ability to add / remove certificates as required by the council.

1.3. Certificates are required for public facing HTTPS websites to encrypt and secure council data.

1.4. The current support and maintenance contract expires 11th September 2018.

2. Main issues

Reason for contracts procedure rules waiver

2.1. Entrust are the councils current provider of SSL Certificate services. Should the council not award the contract to Entrust Limited there will be a significant cost of change in monetary terms and would also create a resource pressure.

2.2. The council currently uses 72 SSL, Unified Communications (UC) and Subject Alternative Name certificates. The council must have an agreement in place with a certified authority to issue these certificates.

2.3. Should the current contract expire a number of Council published web services will be viewed as insecure when accessed via the internet.

2.4. Without an agreement in place there is a significant risk to availability and reliability of key internet published systems together with the potential to damage council reputation.

2.5. Should the contract not be awarded to Entrust the council would incur additional costs to migrate all the SSL certificates to a new provider and resource costs associated with a procurement exercise for a relatively low value contract.

2.6. Moving the service to another provider would lead to a number of council staff requiring training on a different SSL Certificate product range which would incur further additional costs

2.7. Following a review of the market in 2015 and obtaining quotes from various vendors, Entrust were found to offer the best service for the lowest price and the decision was taken to renew the council's agreement with Entrust Limited for SSL Certificates.

3. Corporate Considerations

Consultation and Engagement

3.1. Consultation has taken place with key Digital and Information Services (DIS) stakeholders including DIS Service Development, Security team, Software Licensing and DIS Strategic Sourcing Team.

Equality and Diversity / Cohesion and Integration

3.2. There are no Equality and Diversity / Cohesion and Integration issues associated with this decision.

Council Policies and City Priorities

3.3. The ongoing implementation of SSL Certificates underpins key elements of the Customer Access Programme through modernising the customer experience. The Best Council Plan aims to make the council more efficient and enterprising. Secure web services offered through payments.leeds.gov.uk and functionality on www.leeds.gov.uk support the council in achieving these targets. SSL certificates are a key component of these services.

3.4. SSL Certificates are crucial in allowing secure communications with 3rd parties, present services to the public and for remote working. Examples of services which are dependent on the use of SSL certificates are Adult & Children Social Care systems, VPN, public access planning portal, email and mobile devices.

Resources and Value for Money

3.5. Alternative vendors were considered in 2015 and combined with the cost of change it would be more expensive for the council to change SSL Certificate vendor. Through negotiation Entrust have maintained their pricing from 2015 which will continue to provide value for money to the council.

3.6. Financial provision exists within the approved ICT Operational revenue budget to undertake the action proposed.

3.7. No additional resources are required to implement this decision.

Legal Implications, Access to Information and Call In

3.8. The decision is a Significant Operational Decision and is not subject to call in. There are no grounds for keeping the contents of this report confidential under the Access to Information Rules.

3.9. In terms of transparency, it should be noted that case law suggests that the Council should always consider whether contracts of this value could be of interest to suppliers from other EU member states and, if it could, the opportunity should be subjected to a degree of advertising. It is up to the Council to decide what degree of advertising is appropriate. In particular, consideration should be given to the subject-matter of the contract, its estimated value, the specifics of the sector concerned (size and structure of the market, commercial practices, etc.) and the geographical location of the place of performance.

3.10. In making their final decision, the Chief Digital and information Officer should note the above comments and be satisfied that the course of action chosen represents best value for the Council.

Risk Management

3.11. In the event of changing provider the council would be exposed to a risk of certificates being incorrectly managed during the transition.

3.12. From April 2015 all SSL certificates will be limited to a maximum validity of 39 months (previously a certificate could have a 4 or 5 year validity). SSL certificates have limited validity periods so that the certificate's holder identity information is re-authenticated more

frequently. It is best practice to limit the amount of time that any key is used, to allow less time to attack it. A 3 year contract extension fits with the maximum validity model.

4. Conclusions

4.1. A new contract to be awarded to Entrust Limited for the provision of an Enterprise Account to support and maintain the councils SSL Certificates for a period of 3 years at a total cost of £11,535.36.

5. Recommendations

5.1. The Chief Digital and Information Officeris recommended to approve the waiver of contract procedure rule 8.1 and 8.2 entering into a contract with Entrust Limited for the provision of an Enterprise Account to support and maintain the councils SSL Certificates for a period of 3 years at a total cost of £11,535.36.