

## Renewal of security systems

Date: 7-12-2022

Report of: Head of Cloud and Platform

Report to: Chief Digital & Information Officer

Will the decision be open for call in?  Yes  No

Does the report contain confidential or exempt information?  Yes  No

### Brief summary

Renewal of security systems to provide the following services: -

The intrusion protection system monitors traffic from the internet and from an array of sensors on the internal corporate network. This provides defence in depth to identify and block malicious traffic that has managed to bypass other layers of security.

Provides Anti-Virus detection and remediation across LCC corporate/public access servers, clients and storage arrays, including advanced capabilities for detecting emerging exploits. The suite is also LCC's primary mechanism for controlling access to removable devices like USB sticks.

### Recommendations

- a) Approve the renewal of key information security products for the term of 1 year, thereby maintaining protection of Leeds City Council's line of business applications and associated personal data held under GDPR. The Trellix licenses will be purchased through Bytes under the Software Framework agreement and will cost £110,292.00 for 12 months.

### **What is this report about?**

- 1 This request is to renew LCC's Anti-virus software and Intrusion Prevention System which actively protect the LCC network from being compromised. Without these products and their supporting technologies, it would not be possible to prevent common attacks.

### **What impact will this proposal have?**

- 2 The threat to information systems is growing and Leeds City Council need to maintain their levels of protection in-order-to mitigate the risk of security breaches.
- 3 The renewal of these security systems will help to mitigate potential exploitation of line of business applications and their data.

### **How does this proposal impact the three pillars of the Best City Ambition?**

Health and Wellbeing       Inclusive Growth       Zero Carbon

- 4 Protection of Leeds City Council's line of business applications and associated personal data held under GDPR. These Line of Business applications directly and indirectly support the trinity of 'Health and Wellbeing', 'Inclusive Growth' and 'Zero Carbon'

### **What consultation and engagement has taken place?**

Wards affected:

Have ward members been consulted?       Yes       No

- 5 Not applicable

### **What are the resource implications?**

- 6 There are no resource implications for this as the systems are already in place protecting the data that LCC holds.

### **What are the key risks and how are they being managed?**

- 7 If this proposal was not accepted, it will be necessary to disable all of these security systems thereby leaving LCC exposed to a security breach.
- 8 To highlight this, the recent cyber-attack on Redcar and Cleveland Council left 135,000 people for a period without access to online council services (back to pen and paper), cost £8.7m to remediate and led to significant national reputational damage.

### **What are the legal implications?**

- 9 As the value of the decision contained within this report is over £100,000 but below £500,000 over the 12 month period of the contract this is a Significant Operational Decision and is

therefore not subject to call in. This report does not contain any exempt or confidential information under the Access to Information Rules.

- 10 LCC have a statutory obligation under GDPR to protect people's data that it holds to provide key services. If this data is not adequately protected it is possible for the Information Commissioner to impose significant fines for any ensuing cyber security breach. These systems are in place to directly protect the data from being compromised
- 11 LCC are also required to adhere to the Public Service Network (PSN) Code of Connection (CoCo) in order to access other key governmental systems, including the link to council tax information/funding. Without the security systems in scope of this request it would not be possible to meet the CoCo requirements and therefore share key data with central government. This could prevent LCC from providing services they are legally obliged to offer.
- 12 There is a risk of an ombudsman investigation arising from a complaint that the Council has not followed reasonable procedures, resulting in a loss of opportunity. Obviously, the complainant would have to establish maladministration. It is not considered that such an investigation would necessarily result in a finding of maladministration however such investigations are by their nature more subjective than legal proceedings.
- 13 Although there is no overriding legal obstacle preventing the course of action set out in this report, the above comments should be noted. In making their final decision, the Chief Digital and Information Officer should be aware of the risk of challenge to the Council and be satisfied that on balance the course of action chosen represents Best Value for the Council.

## **Options, timescales and measuring success**

### **What other options were considered?**

- 14 IDS are currently working with technology partners to identify the long-term roadmap for these systems. These assessments will be completed within the coming months with a view to migrating some services away from the current systems as part of LCC's strategy to move to cloud computing.

Any migration from the current systems will require careful planning to ensure that line of business applications are not affected by the transition.

### **How will success be measured?**

- 15 The systems have provided ongoing protection to LCCs IT services with no serious breaches reported to the Information Commissioner due to an attack which these systems would alleviate.

### **What is the timetable and who will be responsible for implementation?**

- 16 These services are already in place, this proposed renewal provides LCC continued use of the products and support in case there are issues e.g. key software patches or new viruses. The licenses that this renewal provides, need to be installed on the requisite systems before they expire on the 31/12/2022

## **Appendices**

- None

## Background papers

- None