Capital and revenue funding - information management and data encryption
Report by: John Blair, Director Corporate Resources

1   Purpose of Report

This report provides an overview on information management and security controls required by the Council to help mitigate future data breaches, allowing for emails to be categorised, encrypted and sent more securely, in line with best practice, to external bodies and individuals and seeks the necessary capital and revenue funding to implement these controls.

2   Background

2.1   The Council has a business requirement to transfer sensitive information to a large number of external bodies and individuals via email and other electronic means. The transfer of sensitive information and data needs to be carried out in a secure manner to prevent sensitive information falling into the wrong hands.

Secure email communication between local and central government, health and criminal justice organisations is possible via the GSX network. However, there is a need to communicate securely on a local level with a large number of voluntary, community sector and private sector partner and providers.

In addition there is a requirement to protect misdirected email correspondence containing sensitive information. It can be fairly easy to accidently send an email to the wrong person or person/s, allowing unauthorised access to the information.

A failure to take appropriate technical or organisation measures to protect sensitive information may result in further breaches of the Data Protection Act and consequential financial penalties.

The IT Services section has carried out initial evaluation of a number of solutions that fulfil these business requirements and allow the secure and controlled transfer of sensitive data to 3rd parties, helping the user categorise the sensitivity of the email before sending. According to the classification chosen, the appropriate level of protection will be applied to the email. Several solutions and products are available that fulfil these business requirements and with the approval of the necessary funding, IT Services would proceed to procure the most appropriate and cost effective solution, following corporate procurement procedures.

2.2 The introduction of the new Information management & security controls will have the following benefits to the Council.
- improved compliance with existing legislation;
- improved awareness of users with regard the nature of the data they are working with;
- protection against council and customer data being sent/accessed by the wrong people;
- protection against potential fines for data breaches; and
- compliance with Information Commissioners best practice guidance.

Report Implications

3.1 Resource

The financial requirements to take forward these planned programmes of work are outlined below:-

Project Description	Capital 2012/13	Revenue p.a. from 2012/13
Data Loss Prevention software Email Encryption & Classification	£60,000	£14,000

These are estimated figures to give an indicative position seeking funding. More accurate details can be provided once the procurement process has been followed.

In addition to the financial commitment above, the implementation of these new information and security controls relies heavily on the buy-in of senior managers and the co-operation of all staff.

3.2 Risk

Failure to enhance our information management and security controls may result in:
- possible non compliance;
- reputational damage; and
- further monetary penalties/fines.

Operational risks associated with these programme streams will be reported through the corporate risk management process and supporting risk registers.

3.3 Policy

Strategy

This project will assist with compliance in relation with the council's acceptable use policy and the wider controls necessary to protect data of the organisation and our stakeholders and customers.

Consultation

No formal consultation is required in relation to this report.

Equalities

An equality impact assessment will be prepared as part of the project.

Sustainability

There are no sustainability implications arising directly from this report.

3.4 IT Issues

There are a number of implications for IT services and service users in delivering this project. Once governance and funding have been agreed projects can be scoped and planned into IT Services work plan.

4 Summary

This project will ensure that the Council enhances the information management and security controls in place to help mitigate future data breaches, allowing for emails to be categorised, encrypted and sent securely in line with best practice to external bodies and individuals. Funding is requested to proceed with procurement and implementation.

5 Recommendations

Council is requested to:-

a) endorse the proposed strategy by approving the technical changes required to implement additional controls in relation to e-mail encryption;
b) allocate a capital budget for procurement of a suitable encryption solution, expected to cost in the region of £60,000;
c) approve a supplementary estimate of £14,000 in 2012/13 and note from 2013/14 onwards an additional £14,000 revenue budget will be required as a revenue consequence of the capital investment; and
d) to note the risks outlined in the report if additional controls are not introduced.

Date: 31 May 2012

Report Contact:
Name: Ian Wragg, Information Security Officer
Tel No: 0131 271 3037 **e-mail:** ian.wragg@midlothian.gov.uk