**POLICY SCRUTINY COMMITTEE** **20 JUNE 2017**

| | |
|---|---|
| **SUBJECT:** | **INFORMATION SECURITY POLICY** |
| **DIRECTORATE:** | **CHIEF EXECUTIVE AND TOWN CLERK** |
| **REPORT AUTHOR:** | **MATT SMITH, BUSINESS DEVELOPMENT AND IT MANAGER** |

## 1 Purpose of Report

1.1 To seek adoption of the updated Information Security Policy.

## 2 Executive Summary

2.1 Information Security remains an important issue for the authority and a key element of this is the adoption and implementation of an Information Security Policy.

2.2 This report provides an updated version of the policy for Members' consideration.

## 3 Background

3.1 ICT Security remains an important issue, and there continue to be high-profile cases reported in the National media. There are many cases ICT systems being compromised including malware attacks or of data being stolen or lost.

3.2 Some examples are:

- The theft of data from 500 million accounts on Yahoo
- Loss of 164m LinkedIn account details
- Theft of 150,000 customers details from TalkTalk(resulting in a £400k fine)
- Malware attacks on Lincolnshire County Council

## 4 Main Body of Report

4.1 A key requirement for ICT Security is to agree and implement an Information Security Policy (ISP).

4.2 Since previous high profile data losses from the Department for Work and Pensions in 2007, Central Government has introduced as assessment process in order for compliant local authorities to access Government ICT services and the Public Services Network (PSN). This process has helped the Council to substantially increase the assurance level in its ICT Security levels.

4.3 An Information Security Policy was previously implemented by the Council in 2009, and due to technological and working practices changes, a review and refresh of the policy is now required. This policy is now presented attached for consideration.

The policy has been written to comply with best practice standards BS7799 and ISO27001. The policy has been subsequently reviewed by internal audit.

The Policy is largely the same as the previous policy, but has been updated to

reflect new technologies and practices. Some detail has been removed where it requires frequent updates and will be provided to employees and Members as necessary in accessible formats.

4.4 Implementing any security restrictions can be inconvenient, costly and an overhead to services; and this policy is no exception. However, the adoption of the policy is recommended as best practice, and although some compromises may be possible, there may also be issues generated with compliance.

4.5 The key elements of the policy are:

- Section 1 – Introduction and linked guidance, policies etc. As the policy is broad in scope and long, detailed guidance is provided that can be updated as technical and operational details change, and can also be provided in more manageable pieces for staff awareness and training.
- Section 2 explains about the policy and how it will be applied and reviewed
- Section 3 outlines and responsibilities with respect to the policy and its implementation. The AD group will oversee its application, with day-to-day activities undertaken by the Business Development and IT Team. However, it is important to note that some responsibility for ICT Security rests with every individual associated with the Council.
- Section 4 relates to ICT and information assets, hardware and software, their ownership and protection.
- Section 5 Provides more information on employee responsibilities, management of ICT Security Incidents and breaches of the policy.
- Section 6 describes the requirements in relation to physical security of ICT Assets, in server rooms, on desktops and remotely.
- Section 7 explains a range of specific control areas, including procedures, changes to ICT infrastructure, malware, vulnerabilities, backup processes, documentation, email, internet usage, compliance with external assessments, and logging of activities. Many of these areas will have more guidance available through documentation provided on the Council's intranet and directly from the Business Development and IT Team.
- Section 8 refers to controlling access to ICT services including user management and technical controls.
- Section 9 outlines controls on development of new systems.
- Section 10 refers to Business Continuity and Disaster Recovery planning for which other plans are currently being developed
- Section 11 explains compliance and audit issues e.g. copyright, data protection (for which there is a full policy) and ICT audit issues.
- Section 12 refers to the Council's disciplinary process for cases in breach of the policy
- Appendices A, B and C provide background information referred to in the document.

4.6 Should the policy be agreed the following steps will then be taken:

- Development and rollout of guidance and awareness sessions for staff and Members.
- Process of signing off with staff and Members to ensure they are aware of their responsibilities.
- Provision of further guidance is ongoing where specific issues arise and will continue to be issued.

## 5 Organisational Impacts

5.1 Finance (including whole life costs where applicable)

Costs can currently be met by existing ICT budgets. However, ICT threats and security are a constantly changing landscape, and it will always be possible to enhance current security levels. Officers will continue to review the position to ensure the Authority has sufficient levels of assurance.

Also, should the Authority fail to mitigate the risks associated with less than optimum ICT security, there is a possibility of fines being imposed, services withdrawn (and subsequent costs) or reputational harm. The authority is obliged to maintain the information it holds in a secure and proper manner.

5.2 Legal Implications including Procurement Rules

5.3 Failure to comply with adequate standards of best practice, could potentially leave the Authority vulnerable to challenges under legislation e.g. Data Protection Act, Freedom of Information Act, RIPA, Criminal Justice and Immigration etc. It has been shown that where positive action is taken to mitigate risks that any subsequent penalties incurred under this legislation will be less severe.

5.4 Equality, Diversity & Human Rights - No equality and diversity implications have been identified in relation to the proposed policy.

## 6 Risk Implications

6.1 (i) Options Explored
ICT Security is important as:

- It protects the organisation from potential reputation harm
- Fines for data breaches are significant
- It is good practice to manage information securely, and is an expectation of the customer
- It supports the delivery of services through shared networks with Central Government
- Without adoption of better ICT Security the Authority is vulnerable to malicious attack, legal action and loss of service.

6.2 (ii) Key risks associated with the preferred approach
As stated above there are significant risks associated with weaker ICT Security levels.

## 7 Recommendation

7.1 The committee are asked to note and provide comments for the Executive to consider.

**Is this a key decision?** No

**Do the exempt information categories apply?** No

| | |
|---|---|
| **Does Rule 15 of the Scrutiny Procedure Rules (call-in and urgency) apply?** | No |
| **How many appendices does the report contain?** | 1 |
| **List of Background Papers**: | Information Security Policy |
| **Lead Officer:** | Matt Smith, Business Development and IT Manager<br>Telephone (01522) 873308 |