Report to Cabinet

Subject: **Update to the Information Security Policy**

Date: 17 December 2015

Author: Research and Development Manager, ICT Support and Council Solicitor & Monitoring Officer

Wards Affected

Not applicable.

Purpose

To seek approval for changes to the Information Security Policy and request delegated powers to approve minor updates or any changes required in order to secure PSN compliance (or equivalent security standard).

Key Decision

This is not a Key Decision.

Background

1.1 Members will recall that the Council's Information Security Policy which was created by the Data Security Group in 2012 and approved by Cabinet 4 April 2013. Members will be aware that the Policy sets out the legal framework for information security along with clearly defined responsibilities. It also includes arrangements for the following:

- Access Controls
- Remote working
- Mobile devices
- Procurement of Systems
- Secure Disposal
- Protective Marking
- Managing security incidents

1.2 The Data Security Group has reviewed the current policy to ensure that it is fit for purpose and has concluded that updates to the Policy are required to meet the continual need to adequately protect the Council's information assets and ensure continued compliance with current guidance/standards.

Proposal

2.1 It is proposed that Cabinet approve the revised version of the Information Security Policy at Appendix 1 to this report. The proposed changes to the Policy fall into 3 categories:

(i) technical changes required in order to maintain Public Services Network (PSN) and Payment Card Industry Data Security Standard (PCI DSS) compliance and reflect current security guidance/standards;
(ii) a re-draft of the Data Management section in order to reflect the revised Government Security Classifications; and
(iii) minor changes to job titles and correction drafting errors.

2.2 In summary the main changes are:

<u>Technical changes</u>

- Expansion of the Payment Card Industry Data Security Standard (PCI DSS) section to include guidance on card handling, Point of Sale terminal configuration and inspection.
- An additional section on Wireless Networking, configuration and use to meet the Payment Card Industry Data Security Standard.
- Changed references to Government Connect to its new name of Public Services Network.
- An addition requirement for Two Factor Authentication for Web Mail access to ensure Public Services Network (PSN) compliance.
- Smartphones and tablets will allow ten attempts to enter the correct User ID and password before wiping the device instead of five, which will increase usability but maintain an appropriate level of security.

<u>Data Management</u>

The current Data Management section classifies the Council's information in 3 categories – Restricted, Protected and Unclassified. These were based on the National Protective Marking Scheme as set out in the Central Government Manual of Protective Security. Since the Information Security Policy was approved, these national classifications have been replaced by the new Government Security Classifications Policy. The Data Management section of the Information Security Policy has therefore been re-written to reflect this as follows:

- All Council information will be classified as OFFICIAL and the previous classifications, RESTRICTED, PROTECTED and UNCLASSIFIED no longer apply,

- There is no requirement to explicitly mark OFFICIAL information, so the previous requirement to mark all information no longer applies,

- OFFICIAL information which is particularly sensitive will be treated as OFFICIAL – SENSITIVE information to denote that it needs additional controls,

- OFFICIAL – SENSITIVE information must be clearly marked to indicate the need for those additional controls,

- The guidance on handling information has been updated to reflect the new classification,

- Special instructions for handing personal data (which is classified as OFFICIAL information) are included to ensure compliance with the Data Protection Act.

2.3 It is also proposed that Cabinet delegate authority to approve regular minor updates to the Information Security Policy or any changes required in order to secure PSN compliance (or equivalent security standard) to the Corporate Director. This will enable Officers to react quickly and ensure the Policy continues to provide a robust framework to protect the Council and the information it holds. Other changes would require Member approval.

Alternative Options

3.1 Not to approve the changes proposed, but this will result in the Policy being out of date and not complying with current guidance/standards.

3.2 Not to give a delegation to the Corporate Director, but this will mean that minor changes to Policy will require member approval.

Financial Implications

4.1 Any costs associated with the implementation of the Policy will be met within existing budgets.

4.2 Compliance with the Payment Card Industry Data Security Standard will ensure that the Council avoids additional fees by Card Processing companies in the region of £5,000 per annum.

4.3 Failure to comply with information governance legislation could result in the Information Commissioner imposing a monetary penalty of up to £500,000.

Appendices

5 Appendix 1 – Information Security Policy v1.5.

Background Papers

6 None identified.

Recommendation

THAT:

(a) The revised Information Security Policy at Appendix 1 to the report be approved; and

(b) The Corporate Director be authorised to approve future minor updates to the Policy or any changes required in order to secure PSN compliance (or equivalent security standard).

Reasons for Recommendations

7.1 To ensure that the Council has a robust up to date policy in place which protects the Council and the information it holds by providing a clear framework for preventing, monitoring and responding to information security breaches.

7.2 To allow ongoing minor updates to the policy to be made by Officers and communicated to all staff as quickly as possible.