# DUNDEE CITY COUNCIL

**REPORT TO:** **Policy and Resources Committee - 14 March 2005**

**REPORT ON:** **Policy on Data and Information Security**

**REPORT BY:** **Head of Information Technology**

**REPORT NO.:** **192-2005**

## 1 PURPOSE OF REPORT

1.1 This report is to seek approval of the committee to implement the attached Data and Information Security Policy within the Council and by doing so to seek compliance with the BS 7799.

## 2 RECOMMENDATION

2.1 That the Committee agree to accept the Data and Information Security Policy Documents in the appendices, and approve the implementation of these throughout the Council.

## 3 FINANCIAL IMPLICATIONS

3.1 The implementation, may result a degree of I.T. expenditure and this will be contained within the I.T. Division Revenue Budget.

## 4 LOCAL AGENDA 21` IMPLICATIONS

4.1 There are no direct local agenda 21 implications.

## 5 EQUAL OPPORTUNITIES IMPLICATIONS

5.1 There are no direct equal opportunities implications.

## 6 BACKGROUND

6.1 The increased use of Technology and especially e-mail and the Internet, has increased the risk of security breaches from outside the council, (eg computer virus attacks), and with the widespread use of internal networked systems, internal threats are also a real consideration. We have for some time had security procedures in place, and these are regularly reviewed and updated, but it has become apparent that I.T. Hardware and Software facilities alone are not enough, and it is now time to implement a formal Information Security Policy.

## 7 CONSULTATION

7.1 Chief Officers and the trade unions have been consulted in the preparation of this report.

## 8 BACKGROUND PAPERS

8.1 None.

D. White
Head of Information Technology

7 March 2005

DUNDEE CITY COUNCIL

# *INFORMATION SECURITY POLICY STATEMENT*

**OBJECTIVE**

The objective of information security is to facilitate business development and maximise stakeholder benefit whilst protecting the Council's information assets from all relevant threats. At all times the cost effectiveness and fitness for purpose of countermeasures will be considered.

Confidentiality - Protecting information from unauthorised disclosure

Integrity - Safeguarding the accuracy and completeness of information and computer software

Availability - Ensuring that information and vital services are available when required

- The purpose of the policy is to ensure business continuity and minimise business damage by minimising the impact of security incidents and, where possible, preventing their occurrence.

- It is the policy of the Council to ensure that:

  - Information will be protected against unauthorised access.

  - Confidentiality of information will be protected.

  - Integrity of information will be maintained.

  - Availability of information will be assured.

  - Regulatory and legislative requirements will be met.

  - Business continuity plans will be produced, maintained and tested.

  - Information security training will be available to all staff.

  - All suspected breaches of information security will be reported to and investigated by the Information Security Officer.

- Procedures have been developed to support the policy.

- The Information Security Officer has responsibility for maintaining the policy and associated procedures and for providing advice and guidance on their implementation.

- All managers are responsible for implementing the policy within their areas of responsibility.

- It is the responsibility of every employee whether permanent, temporary or contract to adhere to the policy.

**SCOPE**

Information assets include hardcopy documents, data, software, storage media, hardware and communications networks.

DUNDEE CITY COUNCIL

# *INTERNET AND E-MAIL POLICY STATEMENT*

OBJECTIVE

To define mandatory practices for the effective and appropriate use of the Internet and e-mail.

- All documents are owned by the Council and not by individuals.

- Use of the Internet and e-mail is primarily for business purposes but limited personal use is allowed consistent with local management requirements. Personal use should generally be limited to lunchtimes or outwith working hours, providing that internet resources are not required for Council business.

- A standard header must be appended to all external e-mail messages, limiting liability and including an appropriate disclaimer.

- The content of e-mail messages and Internet sites browsed or downloaded must not contain anything that could be construed as aggressive, racist, sexist, in poor taste, unsubstantiated opinion, commercially or personally defamatory or otherwise potentially offensive.

- All users must maintain virus awareness.

- All users must ensure compliance with all relevant legislation.

- E-mail folders must be reviewed regularly and any non-essential messages must be deleted in line with the Council's record retention policy.

- All Internet and e-mail traffic, including attachments, and usage of the facilities may be monitored and reviewed and any action deemed appropriate will be taken.

Internet –
refers to the use of any resources from the World Wide Web, whether browsed or downloaded

E-mail –
refers to all use of e-mail whether internal or external

- Procedures have been developed to support the policy.
- The Information Security Officer has responsibility for maintaining the policy and associated procedures and for providing advice and guidance on their implementation.
- All managers are responsible for implementing the policy within their areas of responsibility.
- It is the responsibility of every employee whether permanent, temporary or contract to adhere to the policy.
- The use of Council Internet and e-mail facilities indicates acceptance of the policy.

DUNDEE CITY COUNCIL

# *ACCESS CONTROL POLICY STATEMENT*

OBJECTIVE

Access will be granted in a manner that maintains:

- **The Confidentiality, integrity and availability of information assets**
- **Compliance with legislation**
- **A balance between control and business need**

- All assets will be assigned an Asset Owner who will be responsible for the confidentiality, integrity and availability of those assets (For example, financial records will be owned by the Finance Director)
- Access will only be granted where it is essential for individuals to discharge their responsibilities
- All access will be authorised by the asset owner
- Special controls will apply to the use of privileged access facilities
- Access will be granted, maintained and monitored in a manner that avoids any conflict of interest between those granting the access and system users
- All access rights will be reviewed at a frequency consistent with the business risks
- Managers are responsible for ensuring that the access rights of their staff are consistent with requirements
- Group passwords will not be used
- Passwords shall be selected in accordance with the Policy and Baseline controls manual
- All passwords shall remain confidential to their users
- Wherever possible, transaction accountability will be maintained

SCOPE

This policy applies to all Information assets including data and software, hard copy documents and the buildings within which such assets are stored

- Users shall not leave computer equipment unattended that is logged on with their password
- Remote users shall be authenticated prior to being granted access
- Repeated, unsuccessful logon attempts shall lead to denial of service and subsequent investigation
- Logs of critical system activity shall be maintained for subsequent independent review
- This policy is owned by the Information Security Officer