EAST AYRSHIRE COUNCIL

POLICY & RESOURCES COMMITTEE

4 OCTOBER 2001

PUBLICATION OF THE CORPORATE ICT SECURITY POLICY

Report by the Depute Chief Executive/Director of Corporate Resources

1.0 PURPOSE OF REPORT

1.1 To report progress on the review and update of the Council's Corporate Information and Communications Technology (ICT) Security Policy.

2.0 BACKGROUND

2.1 The Corporate ICT Security Policy defines the policy that will be applied to the implementation, development, management and use of information technology and communications facilities within East Ayrshire Council. The initial Revision 1 of the policy was approved and adopted by the Policy and Resources Committee on 4 December 1997.

3.0 REVISED POLICY

3.1 Revision 2.0 of the Policy addresses the rapid changes in technology and legislation relating to the security of information and covers the period April 2001 to March 2004. It is intended to compliment the Council's Corporate ICT Strategy, Corporate Data Protection Policy and Corporate Data Matching Policy, as well as the Council's e-government strategy. It is supplemented by detailed operational procedures and standards (including the Information & ICT Security User Code of Practice) designed to provide a framework for the safe, secure and legitimate use of ICT within the Council.

3.2 In sections one and two, the policy defines the scope and control mechanisms including the authorisation process for access to ICT facilities and lays a framework for co-operation between other organisations with an interest in ICT security.

3.3 Section three specifies the procedure for allowing access to the Council's ICT systems by other non-Council bodies including contractors. This highlights the need for a written contract with the third party and also deals with access to the Council's Web systems.

3.4 Section four deals with the protection of the Council's physical ICT assets and computer data. It also covers the inventory procedures for the procurement and disposal of assets.

3.5 Section five summarises the risks associated with the use of ICT equipment by Council staff. It addresses the responsibilities delegated to departments for recruitment and training, as well as the procedure for dealing with security incidents.

3.6 Section six covers the physical and environmental security of the Council's data centre and communications infrastructure, including physical access. The section also specifies the insurance cover and the precautions to be taken when equipment is used off-site.

3.7 Section seven addresses the need to document operational procedures. It also deals with change management for new systems, as well as the management of security incidents, audit requirements, capacity management, the use of unauthorised software and the need for backup procedures to ensure the security of data. The section also covers the technical management of the Council's data and communications network.

3.8 Section eight deals with the need to restrict access to systems to only those staff who have a legitimate business need. The section also lays out the procedure to deal with the allocation and resetting of passwords as well as the responsibilities of users. The section refers to the procedure for access to the Council's communications network from home or remote locations, as well as email and Internet access. These procedures are available as separate documents.

3.9 Section nine lays a framework for the project management of installation of new systems, including the use of separate development environments and staff to ensure that live data is kept secure.

3.10 Section ten outlines the managed process to develop and maintain appropriate disaster recover procedures in the event of partial or total equipment failure or as a result of environmental hazards.

3.11 Section eleven outlines the legal context for ICT security and section twelve concludes by highlighting the disciplinary consequences of any breach of the policy.

3.12 The Policy and associated operational procedures will, as far as practicable, address the ICT security management principles defined within BS7799 ‘Code of Practice for Information Security Management’.

3.13 The implementation of the Policy will be managed through ICT Strategy Group (ICTSG), chaired by the Director of Corporate Resources. The group will provide a focus for the implementation and development of the policy within the Council and:

- Ensure that it is formally implemented by all of the Council's constituent departments;
- Review major ICT security incidents, and the exposure to major threats to the Council's ICT systems and infrastructure;
- Provide a mechanism for ensuring adherence to the Policy;
- Provide a mechanism for reviewing the Policy on a regular basis.

3.14 Future revisions will be issued at appropriate intervals. The Head of IT will also be responsible for reporting all potential or actual security threats, and for presenting necessary updates of this Policy to the ICTSG.

3.15 The full document is available for reference at the conclusion of the Committee, with additional copies available to Members on request.

4.0 FINANCIAL & LEGAL IMPLICATIONS

4.1 None.

5.0 RECOMMENDATIONS

5.1 The Committee is asked to: -

i) agree to recommend to Council the adoption of the revised Corporate ICT Security Policy, and
ii) otherwise to note the contents of the report.

Fiona Lees
Depute Chief Executive/Director of Corporate Resources
14 September 2001

LIST OF BACKGROUND PAPERS

Nil

For further information, please contact Malcolm Roulston, Head of Information Technology (01563 576809)

AGENDA