ABERDEEN
CITY COUNCIL

MANAGEMENT OF INFORMATION SECURITY POLICY

Issue 10 – 30th September 2014

DOCUMENT CONTROL SHEET

Issue / Amendment	Date(s)	Pages Amended	Originator	Approved By
Issue 7 (Approved by Continuous Improvement Committee)	21 April 2009	3, 5-10 and 12	ICT Security	R Atkinson
Issue 8 - Updated policy resulting from 2009-2010 Annual Review)	15 March 2010	Front cover and 5-11	RT Guild	S Massey
Issue 8 - to Corporate Policy & Performance Committee for information	29 April 2010	Front cover and 5-11	RT Guild	R Atkinson
Issue 8 - accepted by Corporate Policy & Performance Committee	29 April 2010	Front cover and 5-11	RT Guild	R Atkinson
Issue 9 – to Corporate Policy & Performance Committee for information	20 February 2013	Front cover, 4-5 and 9	RT Guild	S Massey
Issue 9 – accepted by Corporate Policy & Performance Committee	20 February 2013	Front cover, 4-5 and 9	RT Guild	S Massey
Issue 10 – to CMT for approval, change document to an Information Security Policy rather than ICT perspective – as per ICO recommendation.	May 2014	All pages, shown in grey highlight	S Skidmore	S Massey
Issue 10 to Finance, Policy & Resources Committee for approval	30 September 2014	All pages	S Skidmore	FP&R Comm.

Controlled Copy Number:

1 of 1

Document Status:

Final

CONTENTS

1 MANAGEMENT OF INFORMATION SECURITY POLICY

1.1 INTRODUCTION

1.1.1 Aberdeen City Council relies heavily on information, which could be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown in films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected. Information is fundamental to the Council satisfying its corporate governance and legal obligations, the successful operation of its business processes and the delivery of its public services.

1.1.2 As the Council is large and diverse, its information assets must be managed in ways that are efficient and effective; else significant gaps will appear in the Council's defences – thereby jeopardising their ready availability, confidentiality and integrity. All organisations are facing ever-increasing numbers and types of threats; including sabotage, fraud and theft. As more and more organisations link to the Internet, attacks such as computer hacking, spyware and viruses have become increasingly more frequent, sophisticated and targeted. Indeed, there is much more evidence now to highlight a significant trend of attacks originating from within parent organisations.

1.1.3 As the Council increasingly deals with other public and private sector organisations - as well as providing services to the public electronically – it is required to conform to additional standards of acceptable practice as well as meet specific legal obligations. The Council therefore requires comprehensive policies, procedures and standards to be in place to achieve its security objectives, to maintain high standards of service delivery and to fulfil Government's and its own performance targets.

1.1.4 The Council's Information and ICT Security functions supports the provision of the Council's ICT systems and services by ensuring that appropriate and effective administrative and technological protective measures/countermeasures are in place - so as to mitigate the effects of the myriad threats and risks which ultimately jeopardise its data and information.

1.1.5 This management policy is designed to:

a) Be the Council's main management policy for ensuring effective and efficient Information Security throughout the Council and interaction with partners.

b) Support Government's Modernising Government, Efficient Government and Best Value programmes; with particular consideration given to the implications for the Council's own continuous improvement initiatives.

c) Align with the requirements of ISO/IEC 27001 and 27002 (the Information Security Management System industry-standards which all Government organisations are now obligated to comply with).

1.1.6 Appendix A hereto explains terminology that may not be familiar to all of those to whom this policy applies.

1.2 REVIEW

1.2.1 This policy is to be reviewed annually and when otherwise required; and updated as necessary.

1.3 SCOPE

1.3.1 This policy specifies the required involvement, by Council management, to ensure that important information security issues are considered at appropriate levels, in order to give authority and direction to the Council's Information Security initiative.

1.4 APPLICABILITY

1.4.1 This policy applies to:

a) The Council's Corporate Management Team (CMT);

b) Elected Member Group Leaders;

c) Heads of Services;

d) Information and ICT Security Teams, Customer Service and Performance, Corporate Governance;

e) Service Managers (3rd and 4th tier) and equivalents.

1.4.2 It is important to note that subsequent to management decisions being taken which affect Information Security policy, they then need to be considered in detail – with this policy and the corporate ICT Acceptable Use Policy (ICT AUP) & Elected Members' own ICT AUP being reviewed and revised in keeping with such decisions. This requires the combined involvement of Human Resources, Legal and Democratic Services and the Information and ICT Security staff to formulate such policy prior to formal consultation with Elected Members, senior management and trades unions (with the subsequent need to submit new or changed policies to the Finance, Policy and Resources Committee for approval).

1.5 CURRENT THREAT SCENARIO

1.5.1 As alluded to above, all organisations are facing ever-increasing numbers and types of threats. As more and more connect to the Internet, attacks have become increasingly prevalent, malicious and targeted. There is also greater evidence highlighting the potential for attacks to originate from within parent organisations.

1.5.2 Whilst the corporate ICT Security Strategy provides the actual detail about the main (including more prevalent) electronic threats, the following highlights their overall implications for the Council:

a) Disruption to business processes and public services.

b) Non-compliance with legal and regulatory obligations.

c) Breaching of Council-owned intellectual property rights (as-and-where appropriate).

d) Damage to partner, customer and employee confidence.

e) Damage to the Council's reputation, with the potential for significant increases in cases of litigation.

It should therefore be evident that complying with the Council's legal & regulatory obligations and its own corporate governance ones will help minimise the threats which its information systems, ICT infrastructure and electronic information are exposed to.

1.6 PRINCIPLES

1.6.1 The following principles give scope, justification, and determine the need for, management consultation and direction on important matters of an Information Security nature – with the principles being largely derived from BS ISO/IECs 270001 and 27002 (the composite 'Information Security' industry standard for accessing/using and managing organisations' data and information, in keeping with the requirements of their respective ICT AUPs) and sound business practice:

a) Establish corporate and cross-Service management fora to actively promote, guide, review and/or co-ordinate the implementation of appropriate security measures.

b) Use logical, physical, procedural and personnel controls to protect information assets of the Council, its staff and its customers from unauthorised or accidental disclosure, modification, denial of access, misuse, loss or destruction and harm.

c) Limit the use and sharing of data and information to authorised users only, in accordance with best practice and legal & regulatory compliance.

d) Use security risk management techniques, taking due account of information classification requirements, to establish the threats and risks to information assets, and adopt cost efficient and operationally effective solutions to remove or reduce the risk.

e) Develop, maintain and operate secure information and ICT systems to support the integrity of services to customers.

f) Prevent the infection and spread of malicious software (which includes such things as computer hacking, spyware and viruses) on ICT computer and data communication systems and networks.

g) Develop, test and maintain Service continuity plans to remove or reduce the likelihood, impact on and consequences for the Council's business of any disruption to its information and ICT systems and networks, premises or personnel.

h) Ensure Information Security is always a consideration in the evaluation and placing of contracts with suppliers.

i) Promote awareness of Information Security amongst the Council's employees, workers and agency staff', contractors and suppliers (as appropriate); through communication of policies, standards, procedures and guidelines & through ICT User training and general awareness training campaigns.

j) Promote a culture of proactive breach and incident reporting and logging.

k) Periodically monitor and review the effectiveness of the Council's Information Security policies, reviewing and revising them as necessary, in order to ensure their on-going relevance and effectiveness.

l) Maintain the effectiveness of Information Security protective measures/countermeasures by:

i. Taking clear cognisance of the Council's business objectives;

ii. Ensuring that they are appropriate to, and support, the Council's business needs;

iii. Ensuring that they remain cost efficient and operationally effective;

iv. Ensuring that they enable compliance with related legal, regulatory and corporate governance requirements - with particular emphasis on the following (as a minimum) and any amendments thereof:

Local Government (Access to Information) Act 1985. This places a duty on local authorities to actively publish certain information, although there are categories of information which are exempt. It is also of note that some information which was previously categorised as confidential at the time the Act was published may now have to be disclosed under the Freedom of Information (Scotland) Act 2002 as the sensitivity of certain subjects can reduce dramatically over time.

Copyright, Designs and Patents Act 1988. This deals with copyright and intellectual property rights and what constitutes their contravention.

Computer Misuse Act 1990. This deals with unauthorised access to and modification of computer material (with such practices being criminal offences, particularly in respect of electronic information). The Act also deals with the need to securely dispose of such computer material when it is no longer required for its intended purpose(s) by those who are/were authorised to have access to it.

Copyright and Rights in Databases Regulations 1997. Essentially as per Copyright, Design and Patents Act legislation, but including non-authorised modification to databases (which are also subject to copyright and intellectual property rights' ownership).

Data Protection Act 1998. This relates to implementing measures that will ensure the relevance, need for retention, accuracy, integrity and control over the use, handling and disclosure of personal information (although there is other legislation which can take precedence over the disclosing of personal information).

Human Rights Act 1998. This, from an ICT Security perspective, is essentially to do with the following employees' rights:

- Respect for their private correspondence (Article 8).
- Their freedom of thought, conscience and religion (Article 9).
- Their freedom of expression (Article 10).
- Their right of association and Trade Union membership (Article 11).
- Prohibition of discrimination in their enjoyment of Convention rights (Article 14).

Regulation of Investigatory Powers Act 2000. This relates to surveillance or covert monitoring that has taken place, in support of specifically authorised investigations only (as might be initiated by criminal/civil law agencies). An application to undertake a covert surveillance operation requires consideration and an assessment of any potential human rights implications prior to it being authorised.

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. This permits an employer to monitor and intercept communications for specific business purposes, such as; compliance with internal procedures, establishing facts, or to ascertain that acceptable standards are being achieved.

Freedom of Information (Scotland) Act 2002. This is to do with providing non-personal public information on request, subject to specific exemptions.

Local Government in Scotland Act 2003. This, in the context of ICT Security, is essentially to do with Best Value and the need for continuous improvement.

Civil Contingencies Act 2004 and Contingency Planning (Scotland) Regulations 2005. This is to do with having Business Continuity and Disaster Recovery plans in place.

Any other relevant UK laws or directives (particularly as they apply to the Council's Services – individually or collectively)

Any specific security requirements stipulated by the Council's customers and organisations, which provide electronic services to the Council.

m) Routinely monitor, measure and improve the Council's ICT Security measures/countermeasures.

1.7 RESPONSIBILITIES AND ACCOUNTABILITIES

1.7.1 The primary responsibilities and accountabilities for managing Information Security throughout the Council (taking account of all relevant public partnership and other such obligations or requirements) is based essentially on the following:

a) Corporate Management Team (CMT). To give consideration to all referred major issues that have corporate-wide implications, deciding and advising actions which need to be taken in the corporate interest.

The Head of Customer Service and Performance will normally bring such issues to CMT's attention.

b) Elected Member Group Leaders and Heads of Service. To oversee the implementation of Information Security within their respective areas (devolving responsibility to their Service Managers (where appropriate)).

c) Service Managers. To ensure that:

- They are aware of their obligations under this policy and those of the corporate ICT Acceptable Use Policy.
- Staff for whom they have day-to-day line management responsibility are made aware (via team briefings/meetings) of their obligations in respect of the corporate ICT Acceptable Use Policy and its obligations and any additional ones which might arise from periodically published Information Security guidance/advisories.
- They encourage a culture of proactive incident reporting and logging with their staff.
- They and their staff undertake appropriate Information Security awareness learning as may be required from time-to-time (in order to improve their individual knowledge and understanding of what the Information Security 'threat' entails, so enabling them to work more securely).
- Their individual Head of Service and the Information Security Officer/ICT Security Team staff are advised of issues of specific concern.

d) Head of Service Customer Service and Performance.

- Act as the Senior Information Risk Officer (SIRO).
- To give initial consideration to all major issues prior to any report being submitted for CMT consideration, and to provide direction on issues which do not require CMT's involvement.
- To ensure that the Information Management Advisory and Governance Group meets on a routine basis to address all major issues which have significant adverse implications for the access to, use of and delivery of Information and ICT systems and/or services, and the protective measures/countermeasures associated with the continuing availability, confidentiality and integrity of the Council's electronic data networks, computer systems and/or services and data & information.

e) Information Security Officer. To ensure that the Council's Information Security initiative remains relevant, efficient and effective by:

- Keeping the Information Security Management System (ISMS) aligned with the requirements of ISO/IEC 27001 & 27002 and the Council's corporate governance, legal, business objectives or needs & productivity/performance obligations & requirements.
- Keeping the ISMS and technological protective measures/ countermeasures relevant (in conjunction with the ICT Security Team), efficient and effective in order to adequately protect the Council against the threats and risks which its ICT data networks, computer systems and/or services and electronic data & information are exposed to.
- Ensuring that all Information Security breaches and incidents are addressed as timely as the related threats and risks justify.

APPENDIX A - GLOSSARY OF TERMS

ISO/IEC 27001 and 27002: these comprise the combined international standard that sets out the requirements for Information Security Management Systems. It helps identify, manage and quantify the range of threats to which information is regularly subjected. The key controls covered by the standard include:

- **Security policy** - providing management direction and support for information security
- **The organisation of information security** - to help manage information security throughout the organisation
- **Asset management** - to help identify assets and appropriately protect them
- **Human resources security** - to reduce the risks of human error, theft, fraud or misuse of facilities
- **Physical and environmental security** - to prevent unauthorised access, damage and interference to business premises and information
- **Communications and operations management** - to ensure the correct and secure operation of information processing facilities
- **Access control** - to control access to information
- **Information systems acquisition, development and maintenance** - to ensure that security is built into information systems
- **Information security incident management** – to ensure information security events and weaknesses are communicated in a manner allowing timely corrective action to be taken
- **Business continuity management** - to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters
- **Compliance** - To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations, and any additional organisation-specific security requirements