Aberdeenshire COUNCIL

INFORMATION SECURITY POLICY

Scope

The purpose of this Policy is to safeguard information used by Aberdeenshire Council within a secure environment. The objective of information security is to ensure the confidentiality, integrity and availability of information assets through the implementation of controls and through other related policies, procedures and codes of practice.

Policy Statement

We are committed to information security and understand that it is critical to the effectiveness of Aberdeenshire Council and to the level of trust in the Council. It is also critical to those who are associated with us and with whom we share information.

In particular Aberdeenshire Council will ensure that: -

- Information is available to those who legitimately require it.
- Information is protected from unauthorised access or misuse.
- Confidentiality of information will be assured.
- Accuracy and completeness (the integrity) of information will be maintained.
- Regulatory, contractual and legal requirements will be complied with.
- Information security codes of practice and procedures will be developed and applied.
- Operational responsibilities will be identified and observed.
- Employees and others will be briefed and trained in good information security practice.
- Information and information system assets will be classified and protected as required.
- Appropriate controls of the physical, information processing and data communications environment will be maintained.
- Risks to information and information processing will be assessed and contingency plans developed and tested within the wider context of business continuity planning.
- All information security incidents (for example, breaches, threats, weaknesses or errors) will be reported to the Principal Information Security Officer, and investigated through the appropriate management channel.
- Infringement of this Policy may result in disciplinary action. Additionally, where a law may have been broken legal advice will be taken.

It is the responsibility of each employee and information user within the Council to adhere to this Policy.

The Council's Line Managers are responsible for implementing this Policy within their functional area. The Chief Executive has overall responsibility for its implementation. The Policy and Resources Committee approved this policy April 2005.

The Principal Information Security Officer, working with the Council's Information Security Management Group, has direct responsibility for maintaining this Policy approving associated Codes of Practice and for providing guidance on implementation.

Authorised by: Date: 04/3/15

Jim Savege, Chief Executive

POLICY

Revision Date	Previous Revision Date	Summary of Changes
14th May 2015	04th March 2015	Revision and Distribution sections added.
04th March 2015	-	Approval amended from Colin Mckenzie to Jim Savege

DISTRIBUTION

The approved versions of these documents are distributed to:

Name	Title
Arcadia	Our Council/Information Governance/Information Security

Any copies of these documents out with the distribution list above is uncontrolled.