From mountain to sea

Aberdeenshire COUNCIL

Information Security Policy

Version 2.0

Implementation Date: 15 February 2023

1. Purpose and Scope

1.1 The Information Security Policy *(hereinafter referred to as the "**Policy**")* sets out Aberdeenshire Council's *(hereinafter referred to as the **"Council"**)* approach to information security management. The Policy, and the supporting Information Security Framework set out in Section 3 of this Policy *(herein after referred to as the **"Framework"**)*, is in place to support the strategic vision of the Council and to facilitate the protection of the Council's information and technology services against compromise of the core information security Principles - Confidentiality, Integrity and Availability.

1.2 This Policy and the Framework advocates a holistic approach to information security and risk. This is achieved by identifying and assessing information security threats and developing and implementing a combination of people, process and technology controls to mitigate information security risks according to the Council's defined level of risk and the desired objectives. This Policy is owned, managed and developed by the Council's Information Security Officer *(hereinafter referred to as the **"ISO"**)* on behalf of the relevant Head of Service overseeing the Council's IT function. Any queries or feedback relating to implementation or compliance should be directed to the author of this policy.

1.3 This Policy and Framework applies to:

- everyone within the Council who accesses Council information assets or technology. This includes all staff, Elected Members, contractors, visitors, consultants and any third parties engaged to support Council activity and who have authorised access to any Council information assets *(hereinafter referred to as **"Users"**)*;
- technologies or services used to access or process Council information assets;
- information assets processed in relation to any Council function, including by, for, or with, external parties;
- information assets that are stored by the Council or an external service provider on behalf of the Council;
- information that is transferred from and/or to the Council for a functional purpose;
- third-party, public, civic or other information that the Council is storing, curating or using on behalf of another party;

- internal and/or external processes that are used to process, transfer or store Council information

2. Objectives

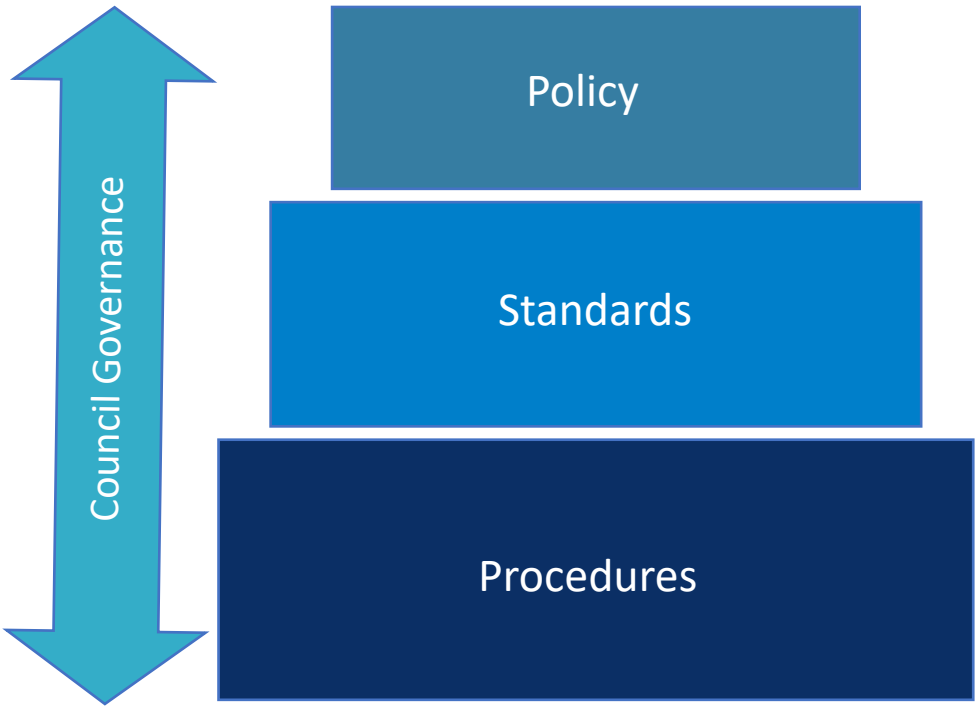
2.1 This Policy and the Framework are designed to:

- promote a holistic approach to information security management;
- protect the Council's information and technology against compromise of Confidentiality, Integrity and Availability;
- support the Council's strategic vision through an approach which effectively balances usability and security;
- facilitate a 'security aware' culture and promote that information security is everyone's responsibility;
- protect the Council's information assets, and third-party data assets being processed or held by the Council on behalf of another party, and technology by identifying, managing and mitigating information security threats and risk;
- define security controls that are effective, sustainable and measurable;
- assist in the compliance of contractual, legal or regulatory obligations;
- identify, contain, remediate and investigate information security incidents to maintain and assist in improving the Council's information security posture;
- develop an informed approach, with regard to information security, in the Users' daily activities across all areas of the Council;
- ensure the Council is compliant with its information security obligations – especially those related to the hosting, curation or processing of third party data;
- provide assurance to other parties that we have a robust control environment in place to protect their data through an effective information security management system;
- ensure we are managing security risks that arise as a result of dependencies on external suppliers and third-party services by ensuring that proportionate and

appropriate security measures to protect systems, services, data, and information have been implemented and form part of our contracts with Service Providers.

3. Framework

3.1. The Council's information security is managed through the below Framework which comprises: (i) this Policy, (ii) Standards and (iii) Procedures, alongside supporting Governance processes. This Framework provides a flexible and effective platform upon which the Council's information security objectives are met. The Framework is detailed below:



Policy: Information Security Policy - *"Why"* - Describes high level objectives and policy statements. Defines why a Policy and Policy Framework is required.

Standards: Information Security Standards - *"What"* - Supplements the Information Security Policy and provides detail on what is required within specific areas.

Procedures: Information Security Procedures - *"How"* - Appropriate procedures to implement the standards. These may be either process or technical procedures and are outcome driven.

3.2. This Policy can be met by adopting and complying with the associated Standards. The Framework is designed to offer flexibility to the ISO in how the outcomes and objectives of this Policy are met, allowing procedural methods and/or controls to be implemented directly by the ISO or relevant IT teams. Everyone within scope of the Policy is required to meet this Policy and associated Standards.

3.3. It is important to note that the Standards, as outlined in associated documentation, must be considered the **minimum** requirements for information security. Where additional information security controls are required for legal, regulatory or governance purposes, the controls must be enhanced accordingly. The ISO can provide advice on how to comply with any additional security requirements, where required.

4. Policy Statement

4.1. The Council manages and produces information that is private, confidential or sensitive in nature, together with information that is regarded as being readily available for general sharing. The Council recognises that it is imperative that all information is protected from compromise of Confidentiality, Integrity and Availability. All within the scope of the Policy **must,** therefore, ensure that:

4.1.1. information assets are, wherever possible, identified, classified and protected. Any security controls which are implemented should be proportionate to the defined classification;

4.1.2. all processes, technology, services and facilities are protected through appropriate information security controls;

4.1.3. information security incidents are identified, contained, remediated, investigated and reported;

4.1.4. where a third party provider or cloud-based system or application is utilised for any services which involve contact with Council information, advice is sought from the ISO before deployment and proportionate and appropriate legally binding assurances in line with the Council's Supply Chain Security guidance are obtained from the Service Provider and their immediate supply chain to keep Council data secure;

4.1.5. an assessment is carried out on all processes, technology, service and facilities in accordance with the associated Standard to manage risks and, where appropriate, approval must be sought from the ISO;

4.1.6. back-up and disaster recovery plans, processes and technology are in place to mitigate risk of loss or destruction of information and/or services and to ensure that processes are in place to maintain availability of data and services;

4.1.7. where off-site working takes place, appropriate security controls are implemented in accordance with the associated Standard.

4.2. In addition, all individuals within scope of the Policy must ensure that reasonable effort is made to protect the Council's information and technology from accidental or unauthorised disclosure, modification or destruction.

5. Compliance / Review

5.1. This Policy and the Framework are reviewed on a periodic basis by the ISO to ensure they remain accurate, relevant and fit for purpose.

5.2. Changes and revisions to this Policy that are required to ensure it remains accurate, relevant and fit for purpose may be made by the ISO without further Committee approval for as long as such changes and revisions do not significantly alter the meaning or essence of this Policy.

5.3. The ISO may carry out periodic compliance and assurance activities (e.g. assessment of security controls) to ensure they are aligned with this Policy and the Framework.

5.4. Failure to meet requirements detailed within this Policy and the Framework may result in the User being subject to disciplinary action that will be dealt with under the appropriate disciplinary code or procedures. Additionally, where it is suspected that an offence has occurred under UK or Scots law (e.g. the Computer Misuse Act 1990), this may also be reported to the Police or other appropriate authority.

6. Responsibilities

6.1. Chief Officers are accountable for ensuring adequate and effective information security controls are in place within their area of responsibility. They are also accountable for compliance in any subsidiary unit within their management - for example schools, leisure centres and libraries.

In addition, the following have Information Security responsibilities:

6.2. The Chief Executive, Directors, Area Managers, Heads of Service and Third-Tier Managers *(hereinafter referred to as* ***"Senior Management"****)* have executive responsibility for information security within the Council. They must actively support the adoption and implementation of the information security requirements, Policy and Framework as well as ensuring compliance within their areas of responsibility.

6.3. System Owners are responsible for maintaining the security of their datasets; setting access requirements for the data; documenting the data made available to other services (either internal or external), and establishing processes to ensure the quality of the data. They have a duty to ensure that data is managed securely and appropriately, that the data is made available only to those people and systems that need access, and that access is provided in keeping with legislation and the Council's internal policies, processes and procedures. If the data includes any personal data, System Owners are also responsible for completing a Data Protection Impact Assessment.

6.4. Users are responsible for protecting the Council's information and technology systems and for complying with this Policy and the Framework. If a User suspects or discovers any material breach of the requirements detailed within this Policy or associated Standards, they must report this to the ISO.

Where an individual User suspects personal data may have been compromised, they must also notify the Data Protection Officer (DPO) through the method detailed within the Data Protection Policy and associated guidance.

7. Associated Standards

7.1. Legislation

7.2. There are a number of pieces of legislation relevant to information security that must be adhered to if the Council is to remain legally compliant when using, storing and handling information. A **non-exhaustive** list of relevant statutory provisions is below:

7.2.1. **General Data Protection Regulation & Data Protection Act 2018** (and any amendment thereof or replacement thereto)

- Both legislation regulate the use of personal data by the Council. Personal data is defined as information relating to a living, identifiable individual and you can access advice and guidance is available on the Council's Data Protection Page.

7.2.2. **Freedom of Information (Scotland) Act 2002** (and any amendment thereof or replacement thereto)

- The Freedom of Information (Scotland) Act 2002 gives individuals a right of access to information held by the Council, subject to a number of exemptions and advice and guidance is available on the Council's Freedom of Information & Environmental Information Page.

7.2.3. **The Regulation of Investigatory Powers (Scotland) Act 2000** (and any amendment thereof or replacement thereto)

- The Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) was introduced to regulate surveillance of a person or persons, and to control information received from third parties when the subject of the activity isn't aware of the surveillance or information gathering. RIPSA also deals with the interception of communications and advice and guidance is available on the Council's Legal & Governance Team.

7.2.4. **Computer Misuse Act 1990** (and any amendment thereof or replacement thereto)

- The Computer Misuse Act 1990 was introduced partly in reaction to a specific legal case (R v Gold & Schifreen [1988] 1 AC 1063 (HL)) and is intended to deter criminals from using a computer to assist in the commission of a criminal offence or from impairing or hindering access to data stored in a computer. The Act contains three criminal offences for computer misuse:

  (1) Unauthorised access to computer material;

  (2) Unauthorised access with intent to commit or facilitate commission of further offences;

  (3) Unauthorised modification of computer material.

7.2.5. **Human Rights Act 1998** (and any amendment thereof or replacement thereto)

- The Human Rights Act 1998 puts the rights set out in the 1953 European Convention on Human Rights into UK law. Article 8, relating to privacy, is of most relevance to information security – it provides a right to respect for an individual's *"private and family life, his home and his correspondence"*.

7.2.6. **Terrorism Act 2000** (and any amendment thereof or replacement thereto)

- The Terrorism Act 2000 (as amended) creates a number of offences in relation to terrorism. Section 19 of the Act imposes a duty on organisations to disclose information where there is a belief or suspicion of a terrorist offence being committed.

7.2.7. **Official Secrets Act 1989** (and any amendment thereof or replacement thereto)

- Staff may be required to sign an Official Secrets Act provision. Unauthorised disclosures are likely to result in criminal prosecution.

7.3. Policies

7.3.1. Social Media Procedure (and any amendment thereof or replacement thereto

7.3.2. Data Protection Policy (and any amendment thereof or replacement thereto)

7.3.3. Use of IT Facilities by Pupils & Students (and any amendment thereof or replacement thereto)

7.4. Supply Chain Security

7.4.1. Security Compliance Standard for Aberdeenshire Council's Service Providers

7.5. Mandatory Codes of Practice

7.5.1. Passwords (and any amendment thereof or replacement thereto)

7.5.2. Acceptable Use (IT) (and any amendment thereof or replacement thereto)

7.5.3. IT Asset Management (and any amendment thereof or replacement thereto)

7.5.4. Information Asset Classification (and any amendment thereof or replacement thereto)

7.5.5. Remote Working (and any amendment thereof or replacement thereto)

7.5.6. Bring Your Own Device (BYOD) (and any amendment thereof or replacement thereto)

7.6. Guidance

7.6.1. Secure Email (and any amendment thereof or replacement thereto)

7.6.2. Mail Procedure (and any amendment thereof or replacement thereto)

7.6.3. Secure Transportation of Paper Records (and any amendment thereof or replacement thereto)

7.6.4. Guidance on Confidentiality (and any amendment thereof or replacement thereto)

7.7. Other Documents and Regulations:

7.7.1. Aberdeenshire Financial Regulations (and any amendment thereof or replacement thereto)

- The Council has made these Regulations in terms of Section 95 of the Local Government (Scotland) Act 1973 which requires every local authority to make arrangements for the proper administration of its financial affairs. These Regulations apply to every employee of the Council or anyone acting on its behalf. In terms of this Policy and the Framework, particular references is made to Para. 5.2.4 of the Regulation which requires that appropriate technical and professional advise must be sought before the expenditure on any I.T. related service.

8. Definitions

8.1. **Confidentiality:** Information is not made available or disclosed to unauthorised individuals, entities or processes.

8.2. **Integrity:** Information's accuracy, validity and completeness is protected. Integrity also covers the concept of non-repudiation where we must be able to prove that we have maintained the integrity of our information, especially in a legal context.

8.3. **Availability:** Information is accessible and usable upon demand by an authorised entity.

8.4. **Threat:** A threat is anything that is capable, by its action or inaction, of causing harm, either directly or indirectly, to a Council information asset. A threat exploits a vulnerability to cause impact to a Council information asset.

8.5. **Control:** Means of protecting the confidentiality, integrity and/or availability of Council information, including policies, standards, procedures, processes or practices, which can be of administrative, technical, management or legal nature. Controls can be detective, preventative or reactive.

8.6. **Information Asset:** A body of information that can be understood, developed or shared and has value to the Council.

8.7. **Information security management:** A systematic approach to managing information within a predefined acceptable range so that it remains secure. It includes people, processes and technology by applying a risk management process.

8.8. **Risk:** The chance or possibility of uncertainty on objectives, expressed as a combination the probability of an event occurring and the impact such an event would have on the achievement of one or more objectives.

8.9. **Contractual obligation:** Requirements set by either the Council or a third party when entering into a contract.

8.10. **Service Providers:** Any legal entity (and its sub-contractors) that provides Services to the Council on a contractual basis.

8.11. **Legal obligation:** Legal requirements, e.g. Data Protection Act 2018 or General Data Protection Regulation (GDPR), Computer Misuse Act 1990. Also, see Para. 7.2 for a non exhaustive list.

8.12. **Regulatory obligation:** Requirements set out by a Regulator, e.g. ICO.

8.13. **Risk assessment:** Structured process for examining information security threats, vulnerabilities and impacts relating to a given system or situation to determine whether an individual control is required or operating as expected.

8.14. **Risk management:** The process of identifying and managing information security risks. Once identified risk are treated by mitigating them, accepting them, transferring them or stopping the process with which they are associated.

— END OF INFORMATION SECURITY POLICY —

Version Control

Version	Date	Author	Description
0.1	28/01/2020	Lars Frevert	Document creation and drafted as a result of Para. 2.1.6 of Internal Audit Report 1932 *"Data Security in a Cloud Based Environment"*
0.2	30/01/2020	Lars Frevert	Draft document updated following feedback and additional research and submitted to ITSMT Decision Board for comment / approval to move forward to the Consultation Stage.
1.0	14/02/2020	Lars Frevert	Following ITSMT Decision Board's approval to move forward to the Consultation Stage in terms of 4B of the Policy Development and Review Framework, draft document submitted to Internal Audit for comment / feedback.
1.1	14/02/2020	Lars Frevert	Draft document updated following feedback from Internal Audit. Updated draft document submitted to Legal & Governance.
1.2	27/02/2020	Lars Frevert	Draft document updated following feedback from Legal & Governance and submitted to HR to progress consultation with Trade Unions and key managers.
1.3	25/06/2020	Lars Frevert	Draft document updated following feedback from consultation with Trade Unions and key managers.
1.4	01/09/2020	Lars Frevert	Draft document placed before Area Committees between 18/08/2020 and 01/09/2020 for review and comment with proposal to replace the current Information Security Policy.
1.5	01/09/2020	Lars Frevert	Draft document updated following feedback from the Marr, Banff & Buchan, Buchan, Garioch, Kincardine & Mearns and Formartine Area Committees with view of placing final document before the Business Services Committee.
1.6	15/10/2020	Lars Frevert	Draft document finalised in order to be placed before Business Services Committee on 12 November 2020 for approval.
1.8	18/02/2021	Lars Frevert	Update to various links contained within the Policy.
1.9	13/06/2022	Lars Frevert	Update to links and review to ensure the Policy remains accurate and relevant. Added Supply Chain Security (Para. 7.4) to the Associated Standards section.
1.9.1	13/02/2023	Lars Frevert	Policy updated to add reference to the Mandatory Code of Practice Bring Your Own Device (7.5.6) and amendment of section 4.1.4 (Policy Statement) to include reference to supply chains management. Change to 4.1.4 was submitted to IT Security Group for review with no comments provided and change was adopted and submitted to Head of Customer & Digital Services on 14/02/2022 for final approval.

Approval

Version	Date	Authority	Approval Comments
1.7	12/11/2020	Business Services Committee	Business Services Committee formally approved the Information Security Policy on 12 November 2020. Information Security Policy (v. 1.7) implemented on 30 November 2020.
1.8	18/02/2021	Information Security Officer	Links update following retirement of the Information Security SharePoint Page and incorporation of same in IT Hub. Updates made pursuant to Para. 5.2
1.9	13/06/2022	Information Security Officer	Annual review of Policy.
2.0	15/02/2023	Head of Customer & Digital Services	Policy update following an internal audit recommendation and inclusion of supply chain management guidance with Policy changes approved by Head of Customer & Digital Services in line with para. 3.3.2 of Part 4B of the Scheme of Governance - Policy Development and Review Framework as well as para. 3.14 Part 2B of the Scheme of Governance List of Officer Powers