# Item: 7

## Asset Management Sub-committee: 7 November 2019.

## Information Security Policy.

## Report by Executive Director of Corporate Services.

# 1. Purpose of Report

To consider the revised Information Security Policy.

# 2. Recommendations

The Sub-committee is invited to note:

### 2.1.

That the Information Security Policy, approved in July 2010, was last reviewed and updated in January 2016.

### 2.2.

That the Information Security Policy has been revised to reflect the current organisation structure, together with changes in both threat landscape and legislative drivers.

**It is recommended:**

### 2.3.

That the revised Information Security Policy, attached as Appendix 1 to this report, be approved.

# 3. Background

### 3.1.

A Data Protection and Information Security Audit was undertaken in 2012 to 2013. Recommendation 1 of that audit stated “All policies should be reviewed in accordance with the requirements stipulated within them. The outcome of these reviews should be reported to Committee”.

### 3.2.

The Information Security Policy, which was originally approved by Council in July 2010, forms a part of the policy suite encompassed by this recommendation.

### 3.3.

Whilst still fit for purpose as a statement of intent, the policy at that time reflected the previous structure of the Council. The policy was subsequently updated, considered and recommended for approval by the Asset Management Sub-committee on 28 January 2016.

## 4. Revised Policy

### 4.1.

Following further changes, the Information Security Policy has now become due for review and update. The Information Security Officer has undertaken the review and has updated it to reflect the current structure of the Council and changes in both threat landscape and legislative drivers.

### 4.2.

The revised policy, attached as Appendix 1, is now submitted for consideration.

## 5. Corporate Governance

This report relates to governance and procedural issues and therefore does not directly support and contribute to improved outcomes for communities as outlined in the Council Plan and the Local Outcomes Improvement Plan.

## 6. Financial Implications

There are no financial implications arising directly from this report.

## 7. Legal Aspects

There are no legal implications arising directly from this noting report.

## 8. Contact Officers

Gillian Morrison, Executive Director of Corporate Services, extension 2103, Email gillian.morrison@orkney.gov.uk.

Hayley Green, Head of IT and Facilities, extension 2309, Email hayley.green@orkney.gov.uk.

Tony Whenman, Information Security Officer, extension 2157, Email tony.whenman@orkney.gov.uk.

## 9. Appendix

Appendix 1: Information Security Policy – August 2019.


# Information Security Policy

**Version 2.3.1**

August 2019

# Contents

# 1.0. Introduction

Information, whether held on electronic information systems, paper, optical storage, magnetic storage, or any other medium represents an extremely valuable asset to Orkney Islands Council (the Council).

The aim of this policy is to establish an operational framework and define officer responsibilities to address organisational information security so that the Council, in providing services to the public, can demonstrate that it will safeguard information held and processed on behalf of its citizens and partner agencies.

Specific controls for the clauses and categories of the ISO 27002:2005 standard will be addressed by an Information Security Management System (ISMS). Detailed operational policy and control documents subordinate to this policy will set out operational standards and requirements. Specific plain language guidance for staff will be made available to all employees, elected members and contractors on request.

## 1.1. The Principles of Information Security

- Ensure confidentiality:
    - That information access is restricted to those with specific authority to view the information and that proper protocols for the sharing of information with partner agencies are in place where this is required and where it is permitted by relevant legislation.
    - To prevent the theft or loss of information and mitigate the associated financial and reputational risk.
- Maximise integrity:
    - Ensuring that all system assets are operating correctly according to specification and particularly in respect of accuracy, security and relevance.
- Maximise availability:
    - Ensuring that data output is delivered to the point where it is needed, when it is needed.

## 1.2. The ISO 27002:2005 Information Security Standard

In order to put in place a framework to publicly demonstrate that equipment and information are adequately protected, and that the integrity, availability and confidentiality of information are safeguarded, the Council will implement the general principles of the ISO 27002:2005 security standard. This provides guidance on the issues which need to be addressed to realise overall information security, including the physical and other threats to information held on electronic systems and other media.

It is intended as a practical framework and provides a Code of Practice, key controls and a specification for Information Security Management Systems, which are a set of operational policies, standards and controls concerned with information security management.

# 2.0. Policy

The Council recognises the importance of protecting the information it holds on behalf of its citizens, employees, Scottish Government and partner agencies and will adopt the ISO 27002:2005 Code of Practice for Information Security Management as the framework for its Information Security Management System.

## 2.1. Applicability

This policy applies to:

- All Council employees, both temporary and permanent, and elected members.
- Staff providing services to the Council under the terms of a service level agreement, contract, consultancy or any other arrangement.
- Staff working in partnership with other organisations. Staff working under these arrangements should be aware that they may also have specific information security responsibilities to the partner organisation.
- Any other contractual arrangement where there is a need to access information systems, manual records and processes.
- Any other third-party users.
- All premises and equipment owned by the Council or any service or equipment provided by a facility management arrangement.

## 2.2. Scope

The scope of this policy includes the 11 information security clauses defined in the standards document ISO 27002:2005. This policy satisfies the first clause. The clauses are:

- Security Policy.
- Information Security Organisation.
- Asset Management.
- Human Resources Security.
- Physical and Environmental Security.
- Communications and Operations Management.
- Access Control.
- Information Systems acquisition, development and maintenance.
- Information Security Incident Management.
- Business Continuity Management.
- Compliance.

Information security operational policy and control documents for each of these clauses will form an Information Security Management System specified in and necessary for compliance with ISO 27002:2005 and subordinate to this policy. Major changes will be presented to the appropriate Council committee as necessary for approval prior to implementation.

The Council document ‘OIC Information Security Staff Guidance’ provides specific guidance on information security and acceptable use of resources and is issued to all staff and elected members that use the Council’s ICT systems.

## 2.3. Legal Framework

Some aspects of information security are governed by legislation. Procedures established under this policy will ensure compliance with the following statutes and regulations:

- The Data Protection Act 2018.
- The General Data Protection Regulation 2018.
- The Computer Misuse Act 1990.
- Copyright, Designs and Patents Act 1988.
- Freedom of Information (Scotland) Act 2002.
- The Regulation of Investigatory Powers (Scotland) Act 2000.
- Human Rights Act 1998.

## 2.4. Corporate Policy Framework

This policy clarifies existing Council policy and rules in terms of information security. It integrates with and supports the following policies forming the Information Governance Framework:

- Records Management Policy.
- Freedom of Information Policy.
- Data Protection Policy.
- Information Security Policy.

The Head of IT and Facilities is responsible for advising the Council on all matters related to information security, in consultation with other officers as appropriate.

All proposed Council policies on information security will be considered by the appropriate Council committee, prior to being adopted by the Council.

## 2.5. Contractual arrangements relating to information security

The terms of this policy should be incorporated into any contract for supplying information systems. This should cover system planning, procurement, acceptance and implementation.

## 2.6. Management and responsibilities

### 2.6.1 Senior Information Risk Owner (SIRO)

The SIRO has overall strategic responsibility for governance in relation to information risks and:

- Acts as advocate for information risk at meetings of the Senior Management Team.
- Provides written advice to the Chief Finance Officer for the Annual Governance Statement relating to information risk.
- Drives culture change regarding information risks in a realistic and effective manner.
- Oversees the reporting and management of information incidents.
- In liaison with the Chief Executive and the Executive Directors, ensures the Information Asset Owner and Information Asset Administrator roles are in place to support the SIRO role.

The Council's SIRO is the Executive Director of Corporate Services.

### 2.6.2. Head of IT and Facilities

The Head of IT and Facilities will:

- Ensure that this policy is implemented, and make recommendations to the Senior Management Team, the Corporate Management Team and the appropriate Council committee when information security policy requirements arise for specific purposes.
- Liaise with the Executive Director of Corporate Services to approve minor changes to this policy under delegated powers.

### 2.6.3. Information Security Officer

The Information Security Officer will:

- Maintain and develop this policy to reflect changes in information security standards, Council structure and national Public Sector security standards.
- Ensure that the Council's Information Security Policy and procedures are kept under review, in order to reflect changing local and national requirements, especially legislation, security standards and national guidance.
- Communicate this policy and monitor the effectiveness of service policies and procedures.
- Develop and manage the corporate Information Security Management System, including operational policies, security standards and controls, outline procedures, security reporting mechanisms and checklists.
- Develop and maintain the information security guidance document issued to Council staff and elected members: 'OIC Information Security Staff Guidance'.
- Monitor the ICT security infrastructure, ensuring compliance with the legislation, standards and guidelines referred to in Section 1 of this policy.
- Monitor and investigate any breaches of information security within the Council.
- Provide an annual report on information security to the Senior Management Team.
- Report any significant breach directly to the Council's SIRO.

### 2.6.4. Executive Directors

Executive Directors will:

- Ensure that staff are aware of their responsibility to comply with this policy and the procedures which implement it.
- Act as Data Controllers for each business process and information system undertaken in their service and monitor their activities.
- Be responsible for implementation of any controls that apply to a system, service or function directly under their control.
- Agree with the Head of IT and Facilities who is to perform the function of System Manager for each information system controlled by the service and supporting its business processes.
- Ensure that all staff with access to any information system read and accept the Use of Computing Resources and the Protection of Information document, and always have ready access to the current release.
- Ensure that this policy and related policies, procedures and information security standards are made available for briefing to all staff.
- Ensure that information security and system training requirements are identified in accordance with the Council's Employee Review and Development Scheme.

### 2.6.5. IT Service Management

IT Service Management will:

- Ensure that mandated controls are in place on all IT infrastructure and exceptions noted where necessary.
- Ensure that the patching policy is implemented, and that patches and updates are applied to systems and appliances in a timely fashion.
- Ensure that all systems are current and in support.
- Ensure that all other technical aspects of the Information Security Management System are in place and monitored.
- Provide evidence of compliance to the Information Security Officer and auditors when required.

### 2.6.6. System Administrators

Each system must have an appropriate Council officer or officers (or contractor) to perform the function of System Administrator for that system. A System Administrator is a member of staff with responsibility for installing, supporting, and maintaining data and application servers, other computer systems or ICT (Information and Communications Technology) infrastructure. The person or people with this function will be nominated by the Head of IT and Facilities or where the system is controlled and managed directly by a service, the relevant Executive Director. The System Administrator for any system must not be the same person as the Data Controller for data contained within the system.

System Administrators will:

- Act professionally and in accordance with the administrator's ethics policy.
- Ensure the efficient functioning and system administration of the system.
- Develop, implement and monitor procedures for the system, satisfying the requirements of the relevant Data Controller, satisfying corporate security standards, using outline policies provided by the Information Security Officer and ensuring compliance with this policy.
- Ensure that procedures are ratified by the Information Security Officer prior to implementation or modification.
- Suspend or deny a user access to the system if the System Administrator suspects that security has been breached, or is potentially at risk; in this event, inform the user's line manager, the relevant Data Controller, and the Information Security Officer.
- Ensure that any user granted access to any part of the system has been authorised by the Data Controller and has read and accepted any standard security guidance on information systems issued by the Council.
- Revoke or adjust privileges in a timely manner when a user leaves the employment of the Council or changes job or responsibilities.
- Ensure that any user granted access to any part of the system has read and accepted any security or acceptable use guidance relating specifically to that system and satisfies the training or knowledge requirements for users of the system.

### 2.6.7. Data Protection Officer

The Data Protection Officer will:

- Ensure, in consultation with the Head of IT and Facilities and the Information Security Officer, that data protection responses do not compromise the security of the Council's data, ICT infrastructure or services.
- Report any significant breach directly to the Council's SIRO.

The Council's Data Protection Officer is the Head of Legal Services.

### 2.6.8. Freedom of Information Officer

The Freedom of Information Officer will:

- Ensure, in consultation with the Head of IT and Facilities and the Information Security Officer, that Freedom of Information responses do not compromise the security of the Council's data, ICT infrastructure or services.

The Council's Freedom of Information Officer is the Information Governance Officer.

### 2.6.9. Information Governance Officer

The Information Governance Officer will:

- Ensure, in consultation with the Head of IT and Facilities and the Information Security Officer, that Information Governance policies support the principles of this

policy in compliance with ISO 27002:2005 and do not compromise the security of the Council's data, ICT infrastructure or services.

### 2.6.10. Individual Employees, Elected Members and Contractors

All individuals to whom this policy applies must:

- Comply with this policy and related policies, security standards and procedures.
- Comply with the guidance to policy given in the document 'OIC Information Security Staff Guidance' or the document 'OIC Information Security for Elected Members'.
- Maintain the highest level of confidentiality regarding information that the individual may come in contact with during the course of their duties in relation to the Council.
- Immediately inform the relevant line manager, the relevant System Manager and the Information Security Officer, if the individual suspects that there has been any security breach.

## 3.0 Non-compliance with Security Policies and Procedures

Any person found to have contravened this policy or the procedures implementing it may face disciplinary action under the Council's Disciplinary Procedure, and / or prosecution under the relevant Act.

## 4.0 Document Control Sheet

Review / approval history.

| Date. | Name. | Position. | Version Approved. |
|---|---|---|---|
| To be confirmed. | General Meeting of the Council. | | Version 2.3.1. |
| | | | |

Change Record Table.

| Date. | Author. | Version. | Status. | Reason. |
|---|---|---|---|---|
| August 2019. | Anthony Whenman. | 2.3.1. | Final. | Reviewed and updated earlier version. |
| | | | | |