Information Security Policy Statement

The Scottish Fiscal Commission follows the Scottish Government's information security policy.

Information is one of the Scottish Fiscal Commission's most valuable business assets and needs to be adequately protected against loss or compromise. This policy has been written to provide a mechanism to establish procedures to protect against the unauthorised disclosure of information. It does not in any way amend the requirements placed upon the Scottish Fiscal commission by the Freedom of Information (Scotland) Act 2002 in relation to the disclosure of official information.

The purpose of this policy is to protect the Scottish Fiscal Commission's information assets from all threats, whether internal or external, deliberate or accidental. This policy covers physical and IT security and encompasses all forms of information such as data stored on computers, transmitted across networks(including websites and social media), printed out or written on paper, sent by fax, stored on removable media such as DVDs and memory sticks, or spoken in conversation and over the telephone. The policy does not seek to prohibit the appropriate sharing of official information with third party agencies, public bodies and other stakeholders.

All line managers are directly responsible for implementing the policy within their business area and for adherence to the policy by their staff and any third parties undertaking work on behalf of that business area.

It is the responsibility of **every staff member** to adhere to the policy. Failure to comply with defined policy and procedures may be treated as a disciplinary offence under the Scottish Government Staff Handbook,

http://saltire/my-workplace/pages/my-workplace.aspx#/Conduct and discipline/Disciplinary procedures and penalties

It is the policy of the Scottish Fiscal Commission to ensure that:

- Information will be protected against unauthorised access[1].
- Confidentiality of information required through regulatory and legislative requirements will be assured.
- Integrity of information will be maintained[2].
- Information will be available to authorised personnel as and when required.
- Regulatory and legislative requirements will be met[3].
- Business Continuity Plans will be produced, maintained and tested.

---

1 Access to all information systems must be controlled as required to ensure that only authorised users have access to the system and its information.

2 Effective precautions must be taken to prevent the infection of Scottish Fiscal Commission computers by malicious software. The latest versions of approved anti-virus programs must be installed on all systems and further updates implemented immediately they are available.

3 Requirements include the Computer Misuse Act 1990, the Copyright Design and Patents Act 1988, the Freedom of Information (Scotland) Act 2002, the Data Protection Act 2018 and the General Data Protection Regulation 2018.

- Information security training will be available to all staff.

- All breaches of information security, actual or suspected, will be reported to and investigated by the Head of Strategy, Governance and Corporate Services[4].

Information on the procedures and mandatory roles and responsibilities in place to support this policy can be found in the Security section of the Scottish Government Intranet.

The Head of Corporate Services has direct responsibility for maintaining the Policy, providing advice and guidance on its implementation. In this role the Chief Security Officer has the right of direct access to the Senior Information Risk Owner (SIRO) and Accountable Officer (AO), which in both cases is the Chief Executive of the Scottish Fiscal commission.

The Governance Manager shall arrange for the Policy to be reviewed bi-annually.

Signed:

Sean Neill

Chief Executive, Scottish Fiscal Commission

Accountable Officer and Senior Information Risk Owner

March 2016
(reviewed April 2021)

Review Log

Agreed by Accountable Officer	March 2016
Reviewed by Governance Board	10 June 2019 25 May 2021
Next review by	June 2023

[4] This includes any event that might have resulted in the loss or potential loss of Scottish Fiscal commission data, information or equipment. Any potential security weaknesses must also be reported.