Information Security Management Policy

Version:	1.4	Status:	Approved
Author/Owner:	Digital Services Manager	Approval/Review:	Audit Scotland Board
Approval Date:	12 April 2018	Review Date:	2 May 2019

Introduction

1. This policy sets out that Audit Scotland will:

   1.1. ensure the confidentiality, integrity, quality and availability of all the information it holds and processes

   1.2. ensure all the information it holds and processes will meet its contractual, legal and regulatory obligations.

2. This policy is supported by supporting policies, standards, procedures and guidance and these are shown in the diagram at Appendix 1.

Scope

3. This policy is mandatory for all employees, contractors and consultants employed by Audit Scotland. Failure to comply with this policy and supporting information security policies may result in disciplinary action.

Commitments

4. Audit Scotland will:

   4.1. produce, maintain and test business continuity plans to ensure the availability of its information and information systems

   4.2. treat information security as a business-critical issue

   4.3. ensure that its information is open and not restricted by financial or legal agreements

   4.4. ensure legislative and regulatory requirements are met (including intellectual property rights)

   4.5. ensure compliance with the General Data Protection Regulation and implement privacy by design in all information systems

   4.6. identify and implement appropriate controls for information assets proportionate to levels of risk

4.7. communicate all appropriate information security policies to all employees, contractors, consultants, clients and other stakeholders

4.8. allocate individual accountability for compliance with all appropriate information security policies, standards, guidance and procedures

4.9. continue to improve its information security management

4.10. develop, implement and maintain an Information Security Management System (ISMS) in accordance with best practice contained within ISO/IEC 27001:2013 and ISO/IEC 27002:2013.

Responsibilities

5. Audit Scotland's Board through its Audit Committee has oversight of risks, including information risks.

6. Audit Scotland's Accountable Officer, with support from the Management Team, has overall responsibility for ensuring this policy is effectively implemented and delivered.

7. Audit Scotland's Senior Information Risk Officer (SIRO) is the Chief Operating Officer, who is responsible for the overall management of the organisation's information risks.

8. Audit Scotland's Management Team will implement and manage appropriate controls to enable conformance to information security policies within their own areas of responsibility and will ensure individual accountability for control performance.

9. The Knowledge, Information and Technology Governance Group (KITGG) will support the Accountable Officer, Senior Information Risk Officer and Management Team by assessing and mitigating information security risks and providing assurance.

10. The KITGG will maintain this policy and associated information security policies ensuring they are communicated, reviewed and updated in response to changes in risks faced by Audit Scotland, legislation, and internal operational working practices.

11. The KITGG will ensure all information security policies and our performance in meeting their requirements is monitored and reviewed on an annual basis.

12. The Digital Services Management Team (DSMT) will maintain information security standards, guidance and procedures ensuring they are communicated, reviewed and updated in response to changes in risks faced by Audit Scotland, legislation, and internal operational working practices.

13. The Corporate Governance Manager is responsible for updating Audit Scotland's Data Protection Policy, managing data subject access requests and providing advice to staff.

14. Information Asset Owners must understand what information is held by their business area, and approve the permissions required to access it.

15. All Managers will be responsible for implementing and communicating appropriate information security policies, guidance and procedures.

16. All employees, contractors and consultants employed by Audit Scotland are required to play an active role in the protection of Audit Scotland's assets and treat information security appropriately in order that this purpose can be achieved.

Change Log

Version	Date	Author	Description
1.0	22/03/16	IT Manager	Information Security Management policy drafted for KITGG approval.
1.1	05/04/16	IT Manager	Some minor changes suggested by the KITGG and policy approved. For submission to the Audit Scotland Management Team for approval.
1.2	15/04/16	IT Manager	Minor changes to reflect Audit Management Team comments. Approved by Management Team and for submission to the Audit Scotland Board.
1.2	05/03/16	IT Manager	Approved by the Audit Scotland Board.
1.3	04/04/17	Digital Services Manager	Minor changes made by KITGG and approved. For submission to Management Team and the Board for final approval.
1.3	05/05/17	Digital Services Manager	Approved by Management Team and Audit Scotland Board.
1.4	12/04/18	Digital Services Manager	Annual effectiveness review and updates made and approved by KITGG. Approved by Management Team on 17/04/18 and Approved by the Board 02/05/18.

Appendix 1 - Information Security Management System Environment