# Information Security Management Policy

| | | | |
|---|---|---|---|
| Version: | 1.7 | Status: | Approved |
| Author/Owner: | Digital Services Manager | Approval/Review: | Audit Scotland Board |
| Approval Date: | MT – 14/09/2021<br>Board – 22/09/2021 | Next review by: | September 2022 |

## 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 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.** treat information security as business critical, whether that be for Audit Scotland information or client data managed by Audit Scotland

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

**4.3.** ensure that its information is open and wherever possible 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 all relevant data protection regulations 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. all information security breaches whether actual or suspected, be reported and investigated in line with approved policies.

4.10. continue to improve information security management

4.11. 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. A monthly cyber security update is scheduled with the SIRO and a member of the Digital Services Management Team (DSMT) that ensures the latest updates are provided to Senior Management demonstrating leadership and commitment to ISO 27001:2013.

9. In addition to the SIRO monthly update, a 6-monthly update on Digital Security is provided to Management Team and then the Audit Committee.

10. 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.

11. 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 through standing agenda items Digital Security and Corporate Risk Register review, both providing assurance.

12. 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.

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

14. The DSMT will maintain the Digital Services Strategy, 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.

15. The Digital Services Team (DST) will deliver the Digital Services Strategy ensuring that all the Audit Scotland's digital systems and services provide an environment that is independent of location, where colleagues can work safely, securely, and effectively, while supporting high quality audit work.

16. The Corporate Governance Manager (CGM) is the designated Data Protection Officer for Audit Scotland, responsible for updating Audit Scotland's Data Protection Policy. In addition, the CGM is the organisation's Records Manager managing data subject access requests and providing governance and compliance advice to staff.

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

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

19. 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. |
| 1.5 | 01/05/19 | Digital Services Manager | Annual effectiveness review by KITGG, Management Team and the Board. Minor changes made to policy. Appendix 1 diagram updated to reflect current ISMS documentation. |
| 1.6 | 13/05/20 | Digital Services Manager | Annual refresh, additional objective included, CGM role updated and removed reference to Cyber Essentials Plus as superseded by ISO 27001. Board approved. |
| 1.7 | 14/09/21 & 22/09/21 | Digital Services Manager | Delayed annual refresh, minor change to responsibilities to include the Digital Services Strategy and Digital Services Team. The Information Security Management System Environment diagram has been updated to include the Secure Build Standard and Asset Management Procedure in the DSMT section. Approved by KITGG on 03/08/2021 submitted and approved by Management Team on 14/09/2021 and then the Board on 22/09/2021 |

## Appendix 1 - Information Security Management System Environment