# Information Security Management Policy

| | |
|---|---|
| **Owned and maintained by:** | Digital Services / Head of Digital Services |
| **Date checked/ created:** | Board approved May 2024 |
| **Next review date:** | May 2025 |

## Introduction

1. This policy sets out that in respect of the information Audit Scotland holds and processes it will have arrangements in place to:

    - protect and maintain the confidentiality, integrity, quality, and availability of all the information it holds and processes

    - manage all the information it holds and processes to meet its contractual, legal, and regulatory obligations.

2. This policy aligns to the Audit Scotland Corporate Plan.

3. This policy is supported by the Information Security Management System documentation shown in the diagram at Appendix 1.

## Scope

4. 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.

5. This policy covers all regulations, legislation and contracts that affect Audit Scotlands information security.

6. This policy is made available to all interested parties.

7. Where appropriate and necessary individual policies state the requirements and processes for handling exemptions and exceptions.

## Information sensitivity classifications

8. Information will be managed in accordance with the Audit Scotland Information classifications as below:

    - Public – Information which has been published or would be readily released under a Freedom of Information (FOI) request

- Controlled – Information that has not yet been published and would require review before sharing with others

- Personal – Information defined as personal data by the UK Data Protection legislation (UK GDPR) and would not be released unless it is lawful to do so. Any information that can identify an individual is defined as Personal.

    - Protected Personal – A sub category of Personal Information that covers sensitive personal information that comprises of:

        - Information classified as "special categories of personal data" under UK GDPR – Race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation.

        - *Detailed unique financial data*, for example a salary or pension amount and *unique identifiers* used for personal life, for example personal mobile number, NI number, Passport Number or Driving Licence number.

## Information Security Objectives

9. Audit Scotland will:

- treat information security as business critical, whether that be for Audit Scotland information or client data managed by Audit Scotland and meet legislative and regulatory requirements (including intellectual property rights)

- seek to ensure the confidentiality, integrity and availability of Audit Scotland's and client owned information, held by, and managed by Audit Scotland

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

- ensure that wherever possible its information is open, not restricted by financial or legal agreements

- comply with all relevant data protection regulations and implement privacy by design in all information systems

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

- manage information security risks to an acceptable level, as defined in the Risk Framework

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

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

- report and investigate all information security breaches, whether actual or suspected and ensure they are reported and investigated in line with approved policies.
- continue to improve information security management and training to raise awareness of the importance of information security regularly to our colleagues,
- develop, implement, and maintain an Information Security Management System (ISMS) in accordance with guidance contained within ISO/IEC 27001:2013 standard.

## Roles & Responsibilities

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

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

12. 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.

13. The Digital Services Management Team (DSMT) ensures the latest updates are provided to Senior Management demonstrating leadership and commitment to ISO 27001.

14. A 6-monthly update on Digital Security is provided to Executive Team and then the Audit Committee.

15. Audit Scotland's Executive 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.

16. The Knowledge, Information and Technology Governance Group (KITGG) will support the Accountable Officer, Senior Information Risk Officer and Executive Team by assessing and mitigating information security risks and threats through standing agenda items on Digital Security and Corporate Risk Register review, both providing assurance.

17. 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.

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

19. 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 practice.

20. The Digital Services Team 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.

21. The Data Protection Officer for Audit Scotland is responsible for updating Audit Scotland's Data Protection Policy, managing data subject access requests, and providing governance and compliance advice to staff.

22. Information Asset Owners must understand what information is held by their business group/teams, and approve the permissions required to access it.

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

24. 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.

## Objectives Evaluation

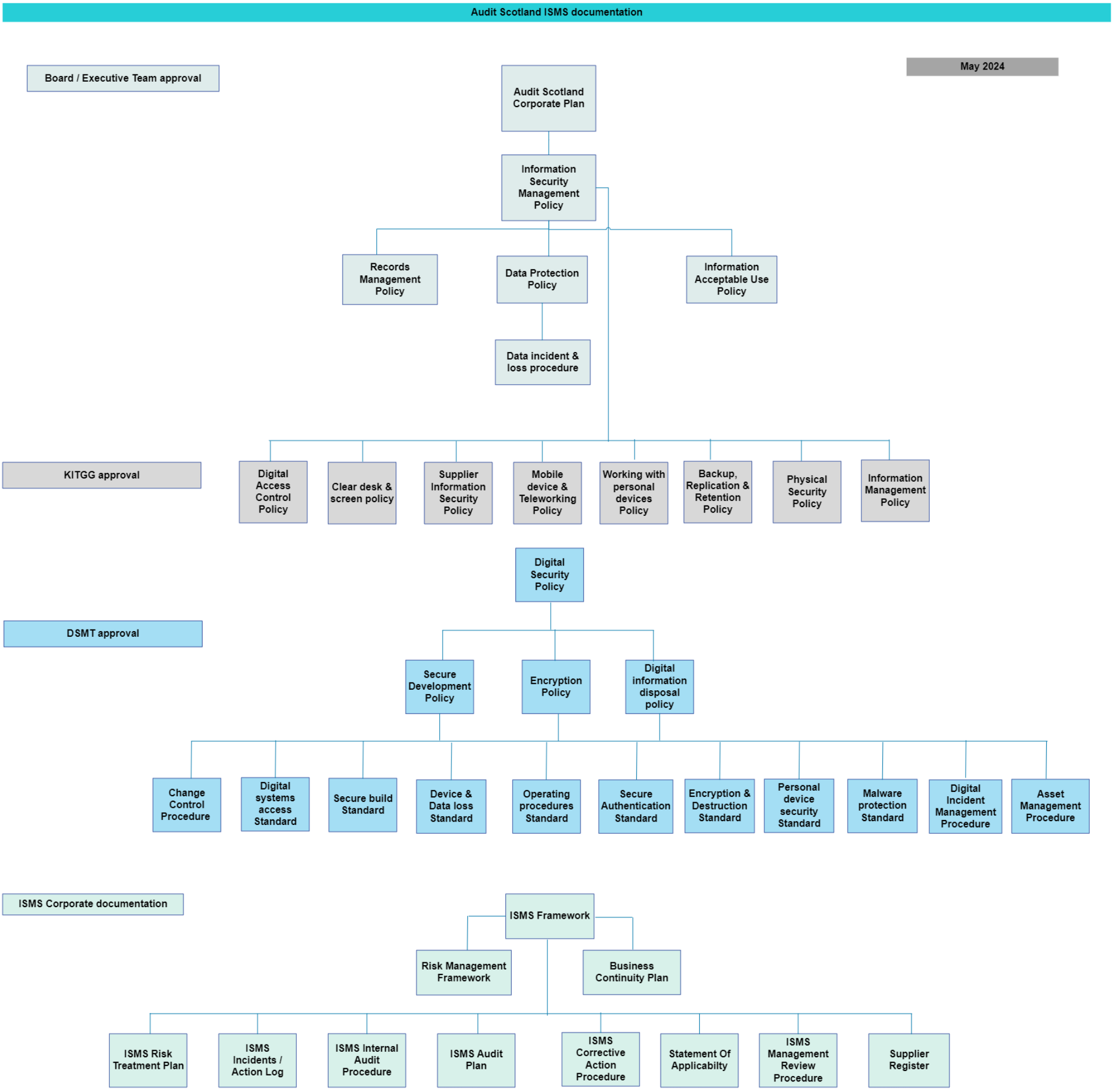
25. Evaluation of our information security objectives in section 10 is reported through KITGG.

## Change Log

| Date | Author | Description |
|---|---|---|
| 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. |
| 22/09/21 | Digital Services Manager | Delayed annual refresh, minor change to responsibilities to include the Digital Services Strategy and Digital Services Team. KITGG and Management Team approved, with final sign off by the Audit Scotland Board on 22/09/21. |
| 17/05/22 | Digital Services Manager | Annual effectiveness review of policy and review timing aligned with all other ISMS documentation. Renamed Commitments section to be aligned with ISMS Framework & Scope. Additional objectives included with an emphasis on risk and raising awareness of information security. ISMS environment diagram updated to reflect document changes. Board approved. |

| | | |
|---|---|---|
| 23/05/23 | Head of Digital Services | Annual review and approval of the policy by KITGG, Executive Team and the Audit Scotland Board. Minor updates made including the addition of a reference to training. |
| March 2024 | Head of Digital Services | Annual review of policy by KITGG in March, then for review and approval by ET and the Board. Updates reflecting compliance with ISO 27001:2013 and the new standard ISO 27001:2022. |
| May 2024 | Head of Digital Services | Approved by Executive Team 08/05/24 and the Audit Scotland Board 21/05/24. |

## Appendix 1


Audit Scotland ISMS documentation
May 2024
Board / Executive Team approval
Audit Scotland Corporate Plan
Information Security Management Policy
Records Management Policy
Data Protection Policy
Information Acceptable Use Policy
Data incident & loss procedure
KITGG approval
Digital Access Control Policy
Clear desk & screen policy
Supplier Information Security Policy
Mobile device & Teleworking Policy
Working with personal devices Policy
Backup, Replication & Retention Policy
Physical Security Policy
Information Management Policy
DSMT approval
Digital Security Policy
Secure Development Policy
Encryption Policy
Digital information disposal policy
Change Control Procedure
Digital systems access Standard
Secure build Standard
Device & Data loss Standard
Operating procedures Standard
Secure Authentication Standard
Encryption & Destruction Standard
Personal device security Standard
Malware protection Standard
Digital Incident Management Procedure
Asset Management Procedure
ISMS Corporate documentation
ISMS Framework
Risk Management Framework
Business Continuity Plan
ISMS Risk Treatment Plan
ISMS Incidents / Action Log
ISMS Internal Audit Procedure
ISMS Audit Plan
ISMS Corrective Action Procedure
Statement Of Applicabilty
ISMS Management Review Procedure
Supplier Register