Information Security Management Policy

Version:	1.3	Status:	Approved
Author/Owner:	DS Manager	Approval/Review:	Audit Scotland Board
Approval Date:	5 May 2017	Review Date:	4 May 2018

Introduction

1. This policy sets out Audit Scotland's strategic commitment to Information Security Management.
2. Audit Scotland will ensure the confidentiality, integrity, quality and availability of all the information it holds and processes.
3. Audit Scotland will ensure all the information it holds and processes will meet its contractual, legal and regulatory obligations.
4. This policy is supported by supporting policies, standards, procedures and guidance. These are shown in the diagram at Appendix 1.

Scope

5. 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

6. Audit Scotland will take appropriate action to ensure the confidentiality, integrity and quality of all the information it holds and processes.
7. Audit Scotland will produce, maintain and test business continuity plans to ensure the availability of its information and information systems.
8. Audit Scotland will treat information security as a business critical issue.
9. Audit Scotland will ensure that its information is open and not restricted by financial or legal agreements.
10. Audit Scotland will ensure legislative and regulatory requirements are met (including intellectual property rights).

11. Audit Scotland will identify and implement appropriate controls for information assets proportionate to levels of risk.

12. Audit Scotland will communicate all appropriate information security policies to all employees, contractors, consultants, clients and other stakeholders.

13. Audit Scotland will allocate individual accountability for compliance with all appropriate information security policies, standards, guidance and procedures.

14. Audit Scotland will continue to improve its information security management.

15. Audit Scotland will 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

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

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

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

19. 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.

20. 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.

21. 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.

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

23. 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.

24. The Corporate Governance Manager is responsible for updating Audit Scotland's data protection notification, managing data subject access requests and providing advice to staff.

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

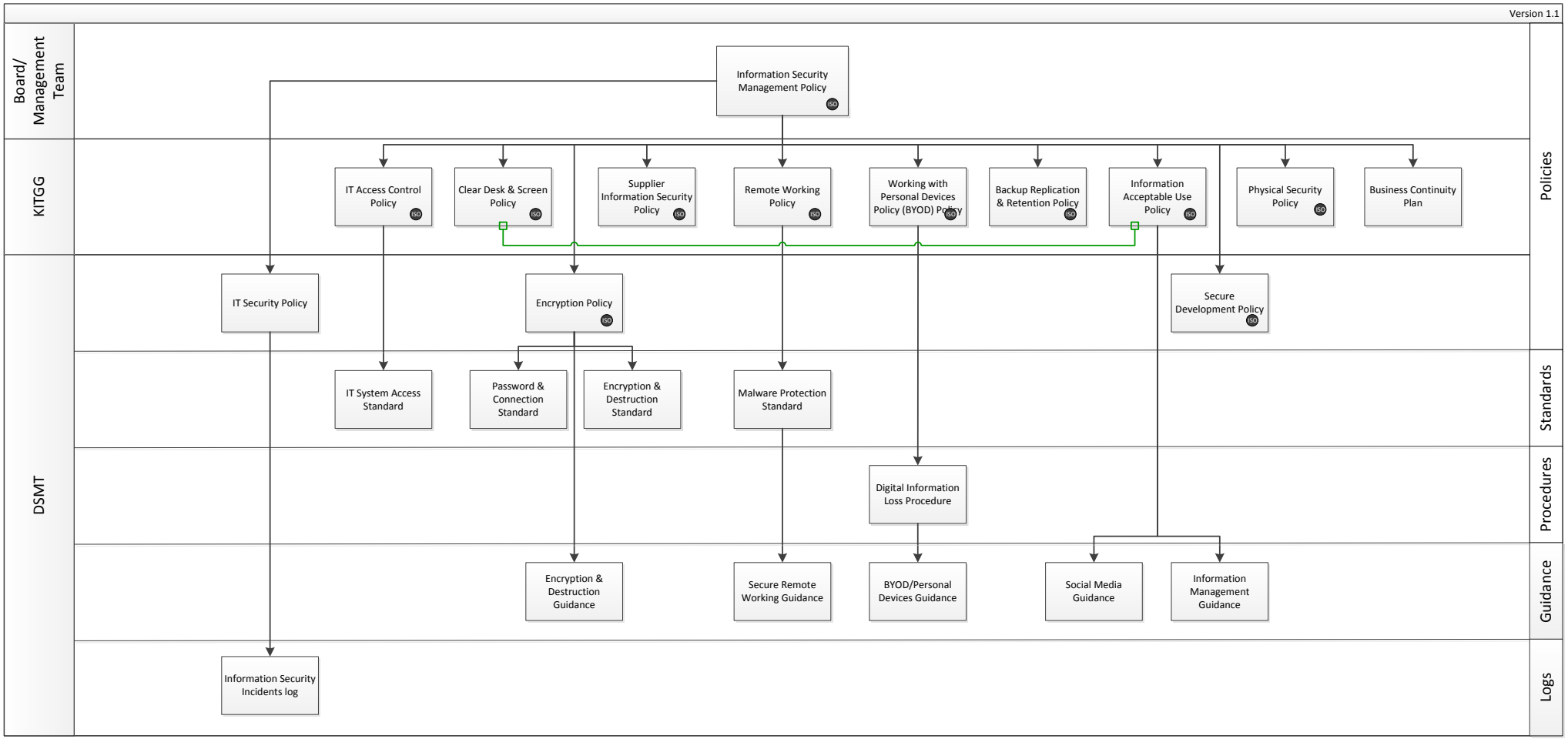
26. All Managers will be responsible for implementing and communicating appropriate information security policies, guidance and procedures.

27. 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	DS Manager	Minor changes made by KITGG and approved. For submission to Management Team and the Board for final approval.
1.3	05/05/17	DS Manager	Approved by Management Team and Audit Scotland Board.

Appendix 1


Version 1.1
Board/ Management Team
KITGG
DSMT
Policies
Standards
Procedures
Guidance
Logs
Information Security Management Policy
IT Access Control Policy
Clear Desk & Screen Policy
Supplier Information Security Policy
Remote Working Policy
Working with Personal Devices Policy (BYOD) Policy
Backup Replication & Retention Policy
Information Acceptable Use Policy
Physical Security Policy
Business Continuity Plan
IT Security Policy
Encryption Policy
Secure Development Policy
IT System Access Standard
Password & Connection Standard
Encryption & Destruction Standard
Malware Protection Standard
Digital Information Loss Procedure
Encryption & Destruction Guidance
Secure Remote Working Guidance
BYOD/Personal Devices Guidance
Social Media Guidance
Information Management Guidance
Information Security Incidents log