Information Security Policy

Version 1.2
Information Security Policy

Title:	Information Security Policy
Classification:	NOT PROTECTIVELY MARKED
Descriptor:	Policy
Policy Reference:	POL/47/05
Summary:	The Agency's approach to compliance with the HMG Security Policy Framework and Information Assurance Standards.
Status:	Final
Version No.:	V1.2
Date Approved:	July 2010
Date of Review:	July 2011
Policy Owner:	Head of Information Assurance
Who to contact for queries:	Information Assurance
Related Policy and Guidance	IA Policy
Audience:	All staff, Delivery Partners and Third Party Suppliers
Reference:	Security Policy Framework DSA Security Policies (see Annex A) HMG Information Assurance Standards (IS1-6) Information Risk Policy Protective Marking Policy and Guidance DSA Information Assurance Strategy

1. Introduction

1.1. This policy is intended to ensure that all data stored, sent or processed by the Agency (or by authorised delivery partners/third parties on its behalf) is protected with a proportionate level of security from events which may compromise its confidentiality, integrity or availability.

2. Purpose

2.1. This Information Security Policy details the Agency's approach to securing data and developing a security-conscious culture throughout the organisation, as well as compliance with legislative and HMG information security requirements.

2.2. Information Security forms a part of the wider Information Assurance function within the Driving Standards Agency. Information Assurance (IA) is defined by the HMG Security Policy Framework as "the confidence that information systems will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users." The DSA gains this assurance through its ongoing programme of IA activities, including the security controls and methods detailed within this policy

3. Scope

3.1. This policy is applicable to all areas of the Agency, including:

3.1.1. administrative staff;
3.1.2. operational staff;
3.1.3. all agency and contractual workers;
3.1.4. all Delivery Partner and Third Party Supplier staff processing information on the Agency's behalf.

3.2. Where this policy reads "DSA staff" or "all staff", it should be read to include the entities above including staff working for Delivery Partners and Third Party Suppliers processing DSA information.

4. Roles and responsibilities

4.1. All DSA staff and any third parties who access DSA sites, systems or data must act in accordance with the contents of this policy. Identifying and reporting potential or realised risks to DSA data, and handling data securely

and in accordance with the HMG protective marking system, are the responsibility of all staff.

4.2. The Agency's Chief Executive will fulfil the role of Accounting Officer (AO); the AO is responsible for approving and signing the Annual Statement of Internal Control, which is then supplied to Cabinet Office. The AO has ultimate responsibility for ensuring that information risks are assessed and mitigated to a level which is acceptable in line with the Agency's stated risk appetite.

4.3. The management of information risk will be owned and represented at board level by the Senior Information Risk Owner (SIRO). The Agency will ensure that the SIRO receives appropriate training for this position.

4.4. The Information Security team will provide advice and guidance to the Agency on security issues. Information Security will maintain an accurate and up to date knowledge base on security issues, and will manage the accreditation and testing schedule for DSA systems.

4.5. The Security Improvement Manager will ensure that standards and guidelines necessary to ensure implementation of, and compliance with, this policy are developed, issued and maintained.

4.6. The Head of Estates & Facilities holds overall responsibility for physical security measures, supported by the Information Security team.

4.7. All line managers are responsible for ensuring that Agency equipment is returned by staff prior to changing role or leaving the Agency, and that access to Information Assets is revoked upon the termination of their employment, contract or agreement.

4.8. Third parties are responsible for supplying evidence of their compliance with HMG security standards and with the contents of this policy, as defined in their contract with the Agency and through the contract management process referenced in the DSA Information Risk Policy.

5. Policy Content

IT Systems

5.1. The Agency will conduct an annual security accreditation project (including a technical risk assessment using HMG IA Standard No.1) for all 'in scope' IT systems. Systems are deemed to be in scope or out of scope for the year's security testing and accreditation schedule through discussion with the Departmental Security Officer (DSO), the Department for Transport's accreditation authority. This results in a risk based decision on the level of testing and accreditation required.

5.2. New systems will be assessed as soon as possible to determine whether they currently (or will once 'live') fall in scope, and will therefore require testing and/or accreditation. This requires involvement from Information Assurance at an early stage in project planning to ensure that projects and programmes are not delayed by security requirements at later stages of development.

5.3. A technical risk assessment is also performed when there is a significant change to existing 'in scope' IT Systems in operation (for example, large changes in functionality, user base or threat).

5.4. The assessment and risk management decisions made are recorded in the Risk Management and Accreditation Documentation Set (RMADS), using HMG IA Standard No.2 - Risk Management and Accreditation of Information Systems; this RMADS is submitted to the Departmental Security Officer for approval. The DSO will assess the security of the system, along with its compliance with IA Standards 1-6, and will award accreditation if the level of residual risk and use of security controls are acceptable.

5.5. In line with the requirements of Information Assurance Standard 6 – Protecting Personal Data and Managing Information Risk, all systems storing or processing data relating to 100,000 or more identifiable individuals will be subject to a penetration test.

5.6. The Agency will seek to reduce the risk posed by technical faults or vulnerabilities identified by technical risk assessments, by working with the supplier to provide adequate mitigation. In the case of systems which are in scope for accreditation, details of the mitigation of these risks will be provided to the Departmental Security Officer along with the test results as part of the accreditation process. If vulnerabilities are identified with systems which are out of scope for accreditation, the Information Security team will provide advice to the Head of Information Assurance and the responsible Information

Asset Owner so that the level of residual risk can be assessed and either accepted or be subject to further mitigation work.

5.7. Third parties which store or process protectively marked DSA data are subject to an assurance and information risk management process which is carried out by the Information Assurance team (for 'in scope' systems, this is in addition to the DSO accreditation). The outcomes of this process are mapped against the Security Policy Framework and Information Assurance Maturity Model to measure compliance to HMG standards.

5.8. Impact assessments are carried out or reviewed on a quarterly basis by designated Information Asset Owners. These assessments use the HMG Business Impact Level tables to assess the risk to the Agency of the compromise to confidentiality, integrity and availability of the data. Conducting this assessment, and taking into account the effect of data aggregation on the resulting impact level, contributes to the adoption and maintenance of a suitably proportionate and secure method of handling the data.

Access Controls

5.9. Access to DSA systems will be granted on the basis of business need ('need to know'). Access controls are specifically to be defined and granted by the relevant IAO.

Protective Marking

5.10. The Agency will maintain and promote compliance with the HMG protective marking system. Guidance on the use of the protective marking system and the handling of protectively marked data will be provided to staff to ensure that information is protected by appropriate controls and technical measures throughout its lifecycle, including creation, storage, transmission and destruction.

Contract Management requirements

5.11. The OGC model contract security clauses will be embedded within all new contracts which use IT systems to store or process protectively marked DSA data.

5.12. The procurement and letting process will ensure that any required Confidentiality or Non-Disclosure Agreements (NDAs) are included in contracts with third parties.

5.13. The DSA will fulfil the requirements of any mandated Code of Connection (CoCo) - for example the Government Secure Intranet (GSI) CoCo - and will provide assurance of its compliance on an annual basis (or more frequently, as required).

Physical Security

5.14. Due to the nature of the DSA physical estate, carrying out an assessment of the security of every DSA building using HMG methodology (eg. SPF Tier 4) would involve expense which is disproportionate to the risk to DSA information; instead, the Agency will carry out a series of physical assessments intended to cover a representative sample of the estate. This will be refreshed at least once every three years. Sites of security breaches or buildings which hold high levels of data will be prioritised for these assessments, and may be audited outside of the three year assessment cycle.

5.15. The physical estate of Delivery Partners and Third Party suppliers must be assessed in line with RMADS procedures, or independently where this is not appropriate.

Business Continuity

5.16. The Agency and its major delivery partners will ensure that Business Continuity and Disaster Recovery plans are in place for all locations where protectively marked information (including cryptographic items) are held. Business continuity and disaster recovery plans will be tested annually at a minimum, with ‘lessons learned’ sought and included in planning.

5.17. The Agency will maintain a Policy Set which fulfils the policy requirements of the Security Policy Framework and IAMM, as detailed in Annex A.

5.18. The Agency will maintain an Information Assurance Awareness Programme, which will provide updates and briefings to staff in order to create and support a culture which values and protects DSA information.

5.19. The Agency will pursue and maintain compliance with all HMG Standards relevant to this policy; for example Information Assurance Standards 1, 2, 4, 5 and 6 published by CESG, and the Security Policy Framework.

5.20. The Agency will maintain compliance with all legislative requirements relevant to this policy, such as the Data Protection Act 1998 and the Computer Misuse Act 1990.

5.21. The Agency will pursue and maintain compliance with commercial security standards which are applicable to its operations, such as the Payment Card Industry Data Security Standard (PCI DSS).

5.22. The Agency will implement a Forensic Readiness Policy, which will detail its approach to maintaining access to appropriate resources for the provision of digital evidence.

Incident Management

5.23. An Information Assurance Forum will draw together staff from Information Assurance and stakeholders from across the Agency to review security matters, promote a security-conscious culture and recommend initiatives designed to promote information security within the Agency.

5.24. Security incidents will be managed by the Head of Information Assurance through the Incident Control Centre and monitored by the Information Assurance Forum; the DSA Incident Management Policy provides further detail.

Culture and Training

5.25. Through methods such as attendance at seminars and conferences as well as subscription to relevant web feeds, the Information Assurance team will monitor ‘best practice’ IA methods and, where it is possible and of benefit to the Agency, seek to implement these practices.

5.26. The effectiveness of the Agency’s security policies and controls will be monitored by the Information Assurance Forum (with input from the Incident Control Centre) and through periodic compliance audits (for example the Security Policy Framework and Information Assurance Maturity Model).

5.27. The Agency will use tools such as periodic staff surveys to measure and monitor the security culture within the Agency, and will use the results of this process to inform future awareness programmes.

5.28. The Agency will ensure that sufficient resources are made available to maintain compliance with the measures and approach detailed within this policy.

6. Revisions and review

6.1. This policy will be reviewed annually by the Information Security Manager (in conjunction with the Security Improvements Manager), or immediately upon the release of new relevant standards, legislative requirements or DSA instigated change.

7. Sanctions and Violations

7.1. Action taken in breach of this policy will be treated as misconduct, and could be seen as gross misconduct. Consequently, the Staff Handbook will apply in all cases going forward for consideration.

8. Annex A

8.1 The Agency's policy set will include the following policy documents (and associated Standard Operating Procedures where appropriate) which will support ongoing compliance with the HMG Security Policy Framework:

- Incident Management Policy
- Clear Desk Policy
- Forensic Readiness Policy
- Counter Eavesdropping Policy
- Acceptable Use Policy
- ICT Disposal Policy
- Removable Media Policy
- Patching Policy
- Content, Malware and Perimeter Management Policy
- Remote Working Policy
- Screening and Vetting Policy

The Agency will ensure there is a programme in place to assess compliance with these policies, and an associated reporting process. Each Delivery Partner and Third Party Supplier will also have policies covering the areas described above to support the DSA contract.