DSA®
DRIVING STANDARDS AGENCY
SAFE DRIVING FOR LIFE

# INFORMATION RISK POLICY

| **Title**: | Information Risk Policy |
|---|---|
| **Classification:** | NOT PROTECTIVELY MARKED |
| **Descriptor:** | Policy |
| **Policy Reference:** | POL/46/03 |
| **Summary**: | Policy on how DSA addresses information risk |
| **Status**: | Final |
| **Version No**.: | 1.2 |
| **Date Approved**: | July 2010 |
| **Date of Review:** | July 2011 |
| **Policy Owner**: | DSA Senior Information Risk Owner (SIRO) |
| **Who to contact for queries:** | DSA Knowledge and Information Management Team |
| **Related Policy and Guidance:** | DSA Risk Policy<br>DSA Information Assurance Strategy<br>DSA Information Assurance Policy Set/Framework<br>DSA Information Security Policy |
| **Audience:** | All DSA Staff, Delivery Partners and Third Party Suppliers |
| **Reference:** | Information Assurance Strategy |

## POLICY SCOPE

1. This policy is applicable to all areas of the Agency, including:
    a. administrative staff;
    b. operational staff;
    c. all agency and contractual workers;
    d. all Delivery Partner and Third Party Supplier staff processing information on the Agency’s behalf.
2. Where this policy reads DSA staff, it should be read to include the entities above including staff working for Delivery Partners and Third Party Suppliers processing DSA information.

## STATEMENT OF INTENT

3. The DSA Executive Board has approved the introduction and embedding of risk management through the DSA Risk Management Policy into the key controls and approval processes of all major business processes and functions of the Agency.
4. DSA recognises that the aim of information risk management is not to eliminate risk totally, but rather to provide the structural means to identify, prioritise and manage the risks involved in all Agency activities supporting the Information Assurance Strategy. It requires a balance between the cost of managing and treating information risks, and the anticipated benefits that will be derived to the business.
5. DSA continues to work to ensure that Government standards on information risk are implemented within the Agency on a day to day basis.

## POLICY OBJECTIVES

6. The Information Risk Management Policy has been created to:
   a. support the maturity of information assurance at DSA & supporting Delivery Partner and Third Party Suppliers' maturity to align with DSA requirements against the Information Assurance Maturity Model (IAMM) and Security Policy Framework (SPF);
   b. provide structure to the implementation of the measures in HMG IA Standard No.6 (Appendix A), and to support the implementation of ISO27001 recommended across Government;
   c. protect the Agency from those risks of significant likelihood and consequence in the pursuit of the Agency's stated strategic goals and objectives;
   d. provide a consistent risk management framework in which the risks concerning business processes and functions of the Agency will be identified, considered, and addressed in key approval, review and control processes;
   e. encourage pro-active rather than re-active management;
   f. promote well managed risk acceptance;
   g. provide assistance to, and improve the quality of, decision making throughout the Agency;
   h. meet legal or statutory requirements;

i. assist in safeguarding the Agency's assets – information, people, finance, property and reputation; and

j. provide an assistive methodology in support of the cultural direction of the DSA, delivered by the IA cultural change plan embodied in the Information Assurance Strategy

k. recognise the need to take a whole life, co-ordinated and systematic approach to IA measures as a whole (not just ICT related) covering information and information systems including plans to determine ongoing IA status.

## STATEMENT OF RISK APPETITE

7. This policy should be read in conjunction with the DSA Risk Policy which identifies the risk appetite of the Agency.

## POLICY STATEMENT

8. DSA adopts the Risk Management approach and general methodology specified in the DSA's Risk Management Policy. All Agency information risk methodology will be based on HMG standards. Specifically, DSA will:

<u>Identify Information Assets</u>

a. Recognise and record all DSA information assets in an Information Asset Register (IAR), including those held by Delivery Partners and Third Party Suppliers. This Register will be kept up to date in line with Departmental requirements, and all assets held by Delivery Partners and Third Party Suppliers will be made clear to them;

b. Identify an Information Asset Owner (IAO) for each asset on the IAR;

c. Each IAO will manage the information risk of the specific asset in line with the IAMM and SPF requirements, and support this with associated documentation appropriate for their business area which will be approved by the Accounting Officer upon the recommendation from the Senior Information Risk Owner (SIRO);

d. The IAR will identify which assets include personal data.

<u>Risk Identification</u>

e. Adopt a process founded on IS1 of CESG requirements of Confidentiality, Integrity and Availability. This ensures there is a consistent approach to the calculation of information risk, and meets the requirements of recognised standards implemented across Government;

ICT System Accreditation

f. Follow an accreditation programme for all ICT systems handling DSA protectively marked information to the Government standard, and to reaccredit such systems when they undergo a significant change, or in line with the requirements from the Departmental Security Officer (DSO);
g. Ensure that Privacy Impact Assessments are conducted in line with project management, accreditation, IAO and data sharing procedures and responsibilities. Such assessments will be used to assess the impact on personal data to support developments within the DSA;

Contract Management

Through the Contract Manager:

h. Ensure that all organisations who handle information on DSA's behalf are assessed to see what parts of this policy are applicable to the processes;
i. Uphold contract management following Office for Government Commerce (OGC) recommended contractual terms and ensure that DSA has a detailed knowledge of information lifecycle and equivalent Governance arrangements relating to roles identified in this policy;
j. Ensure that security requirements inline with the IAMM and SPF are followed by DSA are also followed by organisations (Delivery Partners and Third Party Suppliers) handling information on DSA's behalf and build this into the responsibilities of contract manager and IAOs to monitor this application including agreeing to data sharing activities;
k. Ensure that all risks relating to the contract are captured and informed by contract meetings;
l. Develop an audit plan of Delivery Partners and Third Party Suppliers to report into the Information Assurance Forum and Audit and Risk Management Committee;

Staff Management

m. Ensure all staff, including temporary staff and contractors, are vetted to the appropriate level for their role;
n. Ensure that there is an appropriate level of staff to sustain the work of ensuring information risk is supported within DSA;

o. Manage access control to systems and individual records containing protected personal data;

Strategy and Policy Management

p. Publish and meet the statements made in the Information Charter and ensure it is kept up to date;

q. Ensure that a protective marking scheme is introduced and worked to, including the relevant protective measures in terms of physical and electronic information;

r. Implement and continually review information assurance and management policies;

s. Incorporate information risk considerations into business and strategic planning processes taking the Agency forward;

t. Ensure that there is a Business Continuity Plan (BCP) in place and that this is tested periodically and reported on.

## RESPONSIBILITIES

### Overall

9. Information assurance and identifying information risks is part of everyone’s role at DSA and those handling DSA data on DSA’s behalf. DSA considers all staff in DSA have access to PROTECT personal data

### Governance

10. The DSA Executive Board has ultimate responsibility for the management of risk and the establishment of proper controls as part of its continuing drive to enhance corporate governance in DSA.
11. The Accounting Officer has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level.
12. The Senior Information Risk Owner (SIRO) will be responsible on behalf of DSA for ensuring that an information risk management system is established, implemented and maintained in accordance with this policy.
13. The SIRO owns the Information Risk Policy and information risk assessment. They will act as an advocate for information risk on the Executive Board and internal discussions.
14. The SIRO is responsible for establishing an effective compliance regime to

ensure Information Risk Management measures are put in place and that they comply with endorsed DSA policy.

15. The Audit and Risk Management Committee is responsible for advising the Accounting Officer on the adequacy of audit arrangements (both internal and external) and on the implications of assurances provided in respect of risk and control within the Agency.
16. Internal Audit is responsible for checking that DSA's risk management, governance arrangements and control systems are established and working effectively.

**Operational**

17. The SIRO has delegated responsibility for oversight and implementation of this policy to the Information Asset Owners
18. The DSA Information Assurance Forum (previously Information Security Forum) will support the SIRO and ensure information risk management is embedded in the key controls and approval processes of all major business processes and functions.
19. Daily support to the SIRO is provided by Information Assurance Branch
20. IAOs must satisfy themselves that all action taken by others are effective in discharging their DHR/IS6 obligations, and where they are not, it is the IAOs responsibility to ensure remedial action is taken to increase the efficacy of the measure.
21. Contract Managers and Line Managers of Delivery Partners, Third Party Suppliers and Agency staff will be responsible for their respective areas of business and will be responsible to their respective Information Asset Owner for the implementation and maintenance of appropriate risk management processes. They will provide reports to the IAO as directed on the implementation of the risk management processes. They must ensure that all updates to DSA policies are communicated to DeliveryPartners and third Party Suppliers and that all aspects of the IA Policy Set are included in contract negotiations taking advice from DSA Information Assurance where required.

## ESCALATION AND ANONYMOUS REPORTING OF INFORMATION INCIDENTS

DSA will:

22. Maintain a policy for reporting, managing and recovering from information risk incidents;
23. Maintain up to date and available policy and procedures for incident management in relation to information assets;
24. Ensure there is a mechanism in place that commands the confidence of individuals through which they may bring concerns about information risk to the attention of the relevant IAO, SIRO or the Audit and Risk Management Committee, anonymously if necessary through whistleblowing, and records concerns expressed and action taken in response;

## CULTURE AND TRAINING

25. DSA recognises the importance of having the right culture in place to underpin information assurance and data security so that information risk is understood and efficiently handled in our daily business.
26. There will be an ongoing training and awareness programme/strategy to accompany the implementation of this policy as part of the awareness of information assurance.
    a. All new and existing staff must undertake information risk awareness training on appointment and then at least annually;
    b. All Information Asset Owners must undertake information management training on appointment and at least annually;
    c. The Accounting Officer, SIRO, members of the Audit Committee must undertake and pass, where necessary, strategic information risk management training at least annually;
    d. An awareness programme to ensure that all staff are kept up to date with the requirements of information risk management will be developed and put in place; and
27. Training will be assessed for sufficiency  and effectiveness.Action following this policy should be acknowledged in staff personal development reviews by line management.
28. Further training for specific roles may be required in line with role profiles.

29. DSA has a programme of work to share and learn good practice from others.

## DISCIPLINARY PROCEDURES

30. 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.

## REPORTING/AUDIT

31. Information Asset Owners will provide a written judgement of the security and use of their asset annually to the SIRO. IAOs are also responsible for quarterly and annual risk assessments (or as otherwise necessary) of the confidentiality, integrity and availability of information including the examination of forthcoming potential changes in services, technology and threats. Assessments of availability of information will also take into account Government wide guidance and legal compliance.
32. Information Asset Owners will provide reports to the SIRO on a quarterly, exception basis against IAMM & SPF requirements. IAO's will raise any information risk concerns with the SIRO as appropriate.
33. Information Assurance will provide reports to the SIRO and IAOs on the status of information risk management implementation and the effectiveness across DSA and will periodically report on the identification and assessment of major, strategic risk levels.
34. Annual assessments (self assessment or DSA audit) of Delivery Partners and Third Party suppliers against DSA Policy will be undertaken and reported on to the DSA SIRO in relation to information risk held.
35. The SIRO will provide reports on information risk management to the Audit and Risk Management Committee on a regular basis as required or requested.
36. The SIRO will use reports from the IAOs, Internal Audit and the Chair of the Audit and Risk Management Committee to inform an annual assessment of information risk which must cover the effectiveness of the overarching policy.
37. The SIRO will provide written advice to the Accounting Officer on the content of their Statement on Internal Control relating to information risk.
38. The Accounting Officer (AO) is responsible for signing off the Statement of Internal Control which will cover information risk.

39. The AO will share the relevant material relating to the Statement of Internal Control and the supporting annual assessment inline with DfT Policy.
40. The AO will set out in the annual report summary material on information risk and feed into the Department for Transport's report.
41. Internal audit of processes will be undertaken on direction from the SIRO. Such audits may be at the request of IAOs. Such audits will be reported to the Information Asset Owners concerned and the Audit and Risk Management Committee for any recommendations to be addressed.

Further reporting:

42. A monthly report will be produced for the Departmental Security Officer;
43. The Head of Information Assurance will report into the Audit and Risk Management Committee on the ongoing work being carried out to address information risk. This will include copies of monthly reports to the Departmental Security Officer (DSO). This report will be directed to the Audit and Risk Management Committee and the DSA Executive Board.
44. Information Assurance will report to the SIRO on IA Strategy requirements including the area of culture change.

**Legal and Regulatory Requirements**

45. In managing information risk, DSA will comply with all relevant legislation including the Data Protection Act, Human Rights Act, Computer Misuse Act, PCI Standard and Freedom of Information Act.
46. DSA will also comply with central government security standards and apply Government's minimum standards.
47. In managing information risk, DSA will adopt an information risk management approach consistent with the IAMM, SPF, HMG IS1 Standard and the Information Commissioner's Code of Practice, the Cabinet Office minimum requirements on Information Risk and ISO27001.