CabinetOffice

Guidance on the Department Information Risk Policy

March 2009

Making government work better

Guidance on the Departmental Information Risk Policy

Audience:	**This paper will be of particular interest to Accounting Officers and SIROs**
Action:	**Develop a departmental Information Risk Policy**
Timing:	**Immediate**

Background

1. The Report of the Data Handling Review (DHR) introduced the mandatory minimum standards which require departments to have in place an information risk policy setting out how they will implement the mandatory measures in their departments and throughout their delivery partners and monitor compliance with the policy and its effectiveness.

Guidance on the Information Risk Policy

2. The guidance covers the high level statements that the information risk policy should cover.

Contacts Enquiries about content should be directed to:

dataereviewteam@cabinet-office.x.gsi.gov.uk

Guidance on Information Risk Policy

1. This paper is based on generic IA guidance set out by CESG[1] and published in ISO27002. It is written from the perspective of the requirement of the final report on Data Handling Procedures in Government to protect information, including personal data.

Purpose

2. The information risk policy defines how the organisation[2] and its delivery partners will manage information risk and how its effectiveness will be assessed. In so doing the policy supports the organisation's strategic aims and objectives and should enable employees throughout the delivery chain to identify an acceptable level of risk, beyond which escalation of risk management decisions is always necessary. The policy fits within the organisation's overall business risk framework; information risk need not be managed separately from other business risks.

Policy ownership

3. The management board owns the information risk policy and its implementation. The SIRO is responsible for developing and implementing this policy and for reviewing it regularly to ensure that it remains appropriate to the business objectives and the risk environment. The policy should be published and communicated in a manner that is relevant, accessible and understandable to all employees and relevant external parties, including delivery partners.

Content

4. The policy should include high level statements concerning:

- A definition of information risk and the importance of managing these risks as a means of enabling the effective use of data for the public benefit.

[1] HMG Infosec Standard No 2, Jan 2008. www.cesg.gsi.gov.uk
[2] References to "the organisation" includes its delivery partners

- A statement of intent by management, supporting the business strategy and objectives including where the organisation can only influence its delivery partners.

- The information risk management structure within the organisation with specific roles and responsibilities including the procedures for approving deviations from the policy.

- A threat assessment (or reference to an alternative source where it is inappropriate to publish such information in its totality).

- Information risk management strategy (the organisation's approach to risk appetite, risk tolerance and the sharing of data) and details of the risk assessment methodology.

- The applicable legal and regulatory requirements and the government's minimum mandatory measures and other policies and guidance to be used in the management of information risk covering physical, procedural, personal and technical measures.

- Escalation and anonymous reporting procedures and policy for risk management decisions.

- A plan to introduce the necessary changes in culture to ensure that data is valued, protected and used for the public good.

- Requirements for awareness and training including the corporate and individual consequences of failure to apply the organisation's policies and practices.

- The HR policies associated with failure to adopt departmental procedures on handling sensitive data.

- Minimum requirements for inspections, reviews (internal and external), monitoring and audit.

- External accountability and progress reporting.

- Incident reporting, recovery and contingency policy and procedures.

- Minimum requirements for continuing system accreditation and events that must trigger re-accreditation.

5. The intent set out within the policy should be sufficiently generic to be applicable across the organisation and its delivery partners, whilst providing sufficient detail to ensure consistency across a range of business environments.