

Information Risk Management and Data Handling

To update the Board on progress and issues relating to the Government directives on Information Risk Management and Data Handling

1. Background

The Board agreed to initial actions relating to these matters in June 2008.

Many of the existing controls applied to electronic information and information systems are directed at ensuring the confidentiality, integrity and accessibility of important business information.

The Government is now looking to organisations in the public sector to manage classified information to further ensure that sensitive, restricted, confidential and personal information is dealt with more appropriately and consistently.

Further guidance and instruction has been received from BERR, KPMG and the Cabinet Office on these matters since the Board was last updated.

A document on the subject intended for Board members has been produced by the National Archives and endorsed by Sir Gus O'Donnell. A copy is attached for information.

A statement of internal control on the management of information risk was included in the annual report and accounts for 2007/8. A more detailed statement is prescribed for 2008/9.

2. Progress

2.1 A security forum has been set up by the ICT section which reports to the Head of ICT. The forum deals with information security matters in general and accreditation of any new systems being developed. An initial Information Risk Management and Data Handling policy has been produced.

Staff have been taken through the policy, which relates to the use of removable media and mobile devices, and the policy on supplying classified information to third parties. The policy contains a management process, involving Line Managers and Directors, to be followed where classified information is needed to be issued to third parties.

- 2.2 Encrypted laptops have been rolled out to all but 7 staff, and the work will be completed by October 2008. This protects data in the event of any loss of equipment or an unauthorised access attempt is made, and will allow an easing in the event of the current restrictions.
- 2.3 There has been an amnesty on redundant and surplus removable media. This will be confidentially destroyed, but in the meantime, is kept in a secure location. This has reduced the risk of loss of old data stored within and away from the site. Staff have been instructed to remove classified information from home computers.
- 2.4 Requests to release encrypted classified information are being managed and recorded by the ICT staff.
- 2.5 No further technology controls are seen as appropriate at this time.
- 2.6 These measures do not appear to have had any significant negative effect on operational efficiency.

3. **Issues**

- 3.1 There remains much work and cultural change to implement to meet the Government requirements detailed in the instructions and guidance provided.
- 3.2 The Board will need to agree a strategy and policy for information risk management. The former will be brought to the Board in November 2008, and the latter in December 2008. The heads of terms for the policy are attached for information.
- 3.3 The Board will also need to agree an Information Charter. The draft supplied by the Cabinet Office is attached. Any changes to the draft must be accompanied by a strong supporting case, which may need to be justified to BERR information security officials. A further version will be brought to the Board for consideration at a later date.
- 3.4 Whilst actions to date have addressed electronic data, the directive also relates to paper records. The Authority relies upon the Records Management policy in this regard. The policy will need to be reviewed and updated.

Whilst the culture relating to good records management has improved considerably since the introduction of the Wisdom system, there remains much to do in order to meet the requirements of the directive.

The current classification of records cannot be relied upon for this purpose. This will need to be addressed if a general worst case assumption is to be avoided. Working practices may need to change to more closely match those employed in HR and Finance functions where historically there has been the necessity to have due regard to the nature of the information being

managed for legal reasons. Electronic records held in Wisdom are not classified.

- 3.5 Initially, the business departments will need to provide a classification of their information on a broad basis. Once completed, it should be possible to evaluate the need for any deeper classification and for any further appropriate control measures. This work will need to be completed by November 2008.
- 3.6 Further work will be required to align the policy, terms and conditions of contract, ICT policy, records management policy, procurement policy and performance management system before the end of the financial year. Staff and Board Members will need to be trained in their duties regarding information risk management before September 2009.

A schedule of mandatory measures that are required to be in place to achieve a satisfactory level of control of the risks is attached.

4. **Strategy**

- 4.1 Information risk management should support the Authority's business objectives by ensuring that business critical information and classified records are managed appropriately with respect to confidentiality, integrity, and availability and the legal framework whilst protecting the Authority's reputation.

5. **SHE**

- 5.1 There are no SHE considerations with respect to these matters.

6. **Risks**

- 6.1 Failure to implement the Government's Information Risk Management Directive in accordance with the timetable will lead to embarrassment, loss of reputation with BERR, and an inability to make a compliant statement of internal control in the annual report and accounts for the current year.
- 6.2 Failure to implement necessary controls in an appropriate manner could result in a loss of classified information which could cause embarrassment, a breach of Data Protection Law or breach of contract/confidentiality.

7. Recommendation

The Board is asked to note the risks, the progress to date and to support the approach and note ongoing risk as outlined.

Steve Pennell
Director of Mining Information and Services

September 2008