Policy Documentation:
Information Risk Management Policy (IRMP)

(v3.3)

DOCUMENT PURPOSE:

This policy document prescribes the IRM processes that all Coal Authority staff (including any contractors, consultants or delivery partners working for the Authority) are required to sign acceptance of and adhere to.

- You should also familiarise yourself with the supporting documents found on the Risk Management section of the CA Intranet.

Policy Documentation:
Information Risk Management Policy (IRMP).

Contents:

1.0 What is Information Risk Management (IRM)?

This is the process by which we make sure that the information (both paper and electronic) which is important to the running of our business (information assets) is managed appropriately with respect to its:

- **Confidentiality.**

  We must make sure that we comply with agreements given in contracts or the provisions of UK Law to protect the confidentiality of individuals or organisations we deal with, whilst noting that all information held by the CA may be subject to a request under the Freedom of Information Act.

- **Integrity.**

  We must make sure that the information that is important to our business is accurate in all respects and is managed appropriately to keep it fit for purpose.

- **Access.**

  We must ensure that we can continue to use the information that is important to our business.

The management of information risk requires an appropriate organisational structure with clearly defined roles and responsibilities and that staff to whom these roles are allocated have the appropriate skills and training.

The Authority relies upon its staff, line managers, the Records Management and ICT departments to help manage these risks.

This document seeks to supplement the existing good practices based upon the best practice guidance which HM Government is seeking to embed in every government organisation.

Please note: this policy is applicable to all Authority staff and any contractors, consultants or delivery partners working for the Authority.

I confirm that I have read and understand my responsibilities outlined in Section 1.0: "What Is Information Risk Management"	*Please initial:* **[MR]**

2.0 Governance.

The Authority's Board owns the Information Risk Management Policy and its implementation. Review of the policy and its operation may be undertaken by the Audit Committee on behalf of the Board. The policy will be reviewed at least annually.

The Senior Information Risk Owner (SIRO) is responsible for developing and implementing this policy and for reviewing it regularly to ensure that it remains appropriate to business objectives and the risk environment. The Board has delegated the duties of the SIRO to the Director of Finance and Corporate Services.

This policy will be regularly reviewed and communicated in a manner that is accessible and understandable to all employees, relevant third parties and our delivery partners.

Information risk will be managed like any other risk to the Authority's business and can be raised by anyone in the organisation using the "Information Security Observations" button in our online Service Desk tool, TopDesk. Information risks should also be discussed with your Line Manager, Head of Department (HoD) or Director. In most cases, Line Managers are the departmental Information Asset Owners (IAOs); Line Managers with this role will be notified by the SIRO or HoD.

Information Risk Management (IRM) will be part of the regular departmental risk reviews which will normally be convened by either line managers (IAOs) or departmental Heads. Information risks must be reviewed formally at least every six months, or as directed by the SIRO.

New information risks and any changes to existing risks or information assets (as documented in the Authority's Information Asset Register), will be brought to the attention of the SIRO by the IAOs. These will in turn be assessed by the SIRO with suitable controls defined and agreed between the parties. The SIRO will make recommendations through the Executive Leadership Team (ELT) and the Audit Committee where there are instances of significant new threats or new information assets.

Departmental information risks are debated and moderated by the Security Forum which in turn informs the Audit Committee and then the Board.

I confirm that I have read and understand my responsibilities outlined in Section 2.0: "Governance" *Please initial* **[MR]**

3.0 Training.

The departmental IAOs are responsible for ensuring IRM training is completed by new starters (the successful completion of which is monitored by the Security Forum) during their induction and before formally taking up their post.

It is mandatory for all staff to undergo annual refresher training, details of which will be provided by the SIRO.

- Protecting Information Training on TCA Intranet

In addition, all staff must read and ensure they are familiar with the following information security classification documents which can be found in the Information & Risk Management section of the CA intranet:

- GSC TCA Handling Instructions
- Government Security Classification Presentation
- Desk Aid

I confirm that I have read and understand my responsibilities outlined in Section 3.0: "Training" "	*Please initial* **[MR]**

4.0 Responsibilities and Duties.

Anyone found to be in breach of any of the following responsibilities and may be reported to their line manager or employer and be subject to disciplinary action (eg Employee Disciplinary Policy).

4.1 All Staff: Including Contractors and Delivery Partners.

Information Classification and Marking:

Staff are responsible for making sure that information produced and stored outside of business IT systems, but within WISDOM or network drives, is classified according to the Government Security Classifications illustrated in Appendix 2 of this policy.

You must familiarise yourself with these classification guidelines, in addition to the accompanying TCA handling instructions document for more detailed guidance and examples.

If you require any advice, you should contact your line manager (IAO) in the first instance, or your HoD or SIRO for further clarification.

Storage, Use, Transmission and Disposal:

The storage, use, transmission and disposal of information (in accordance with its classification and marking) must adhere to the security handling rules detailed in Appendix 3 of this policy.

Staff must have the express written permission of their IAO before taking a significant volume of information (either paper records or electronic records on removable media) away from the site.

Further information can be found in Appendix 2: Government Security Classifications

Staff must follow this policy and the attached guidance when handling classified information, irrespective of its source.

Reporting:

Staff must immediately report any breaches of this policy, or any information/security risks either:

- Via the ”Information Security Observation” incident button on TopDesk**.**
- Directly to their IAO / Line Manager.
- Directly to their HoD.

If any member of staff believes that any matter they have raised has not been considered appropriately, then they should escalate the matter to the SIRO. Further escalation should be in accordance with the Authority’s Whistle Blowing Procedure.

4.2 IAO’s and Line Managers

Security:

IAO’s **must** ensure that all classified records are adequately secured in line with their classification and provide adequate lockable storage in the office. IAO’s **must** ensure that classified information is managed and used in line with the Data Handling guidance provided with this policy.

Classification:

IAO’s are responsible for defining the records classification within their own business area, and for ensuring that all staff understand the requirements for records classification.

Authorisation:

IAO’s are responsible for authorising requests from staff to take a significant volume of classified information away from site other than “OFFICIAL – SENSITIVE” or higher classifications which will also require Director level authorisation.

Any variations from the above measures **must** be restricted to those authorised in writing by the Director and must be recorded by the IAO.

The IAO **must** maintain a permanent record of such authorisations within the Wisdom filing system for future review by the SIRO and auditors.

The IAO is responsible for reporting all such variations to the SIRO as they occur.

General:

IAO's are responsible for ensuring that all staff comply with the requirements of this policy in relation to the information assets they are responsible for.

Reporting and Monitoring:

IAO's are to maintain and monitor their own regime and report any breaches, gaps in assurance and positive assurance to their departmental Director and SIRO on an annual basis. Breaches should be reported by all staff using the online service desk's Information Security Observations button as they occur

IAO's are additionally responsible for:

- Ensuring that all staff undergo any training with respect to Information Risk Management as is stipulated by the SIRO.
- Producing a listing of all business information assets including classified records with an assessment of the potential risk to the business in the event of its loss.
- Maintaining this listing and reviewing it on a six monthly basis.
- Reporting any material changes to risks to the SIRO
- Reporting any breaches of this regime or policy to the SIRO and escalating any concerns to the departmental Director or through the Whistle Blowing Procedure.

4.3 Directors.

General:

Directors are to ensure that staff are adequately trained and have the resources to implement this policy.

Directors are to ensure that all staff undergo any training with respect to Information Risk Management as stipulated by the SIRO.

Authorisation:

Directors are to authorise IAO's classifications for business information assets and records as required.

The IAO should escalate to the Director where they have concerns around the handling of a specific information asset, in order to ensure that arrangements for adequate safeguarding are in place, in compliance with the attached Security Handling Rules for Different levels of Protective Marking in Appendix 3.

Directors are to consider requests from IAOs for any variations from the agreed controls outlined in this policy. Any such considerations will be discussed and agreed with the SIRO before being implemented.

4.4 Senior Information Risk Officer (SIRO).

Reporting and Monitoring:

The SIRO is to provide annual reports and assurance on information risk to the Audit Committee, the Board and the CEO as accounting officer (AO).

The SIRO is to deal with all referrals and breaches which require escalation to the Information Commissioner and all communications and reports which the Department (DBEI) may require.

Annual Assurance Report.

The SIRO will provide an annual assurance report to the Audit Committee. The report is to take the following form:

- Governance Statement.
- Material breaches.
- Incidents reported to DBEIS or ICO.
- Whether overall risks to the business have increased or decreased during the year.
- Recommendations for further consideration or action.

Authorisation:

The SIRO is to ensure that any new IT systems undergo an impact assessment and have adequate controls for the management of information assets and classified records.

I confirm that I have read and understand my responsibilities outlined in Section 4.0: "Responsibilities and Duties" *Please initial* **[MR]**

5.0 Forensic Readiness.

Forensic readiness is a discipline which deals with the management of ICT systems which are used to manage information which may need to be produced as evidence in civil and/or criminal investigations is known as forensic readiness.

Threats and risks will be assessed by the SIRO using the government guidelines for threat assessment and guidelines on the need for forensic readiness.

A review will be conducted by the SIRO on an annual basis or when the threats and risks to the business change for any reason.

The Authority's business is subject to the following risks which may require information to be provided in evidence:

5.1 Potential fraud.

- Potential litigation where one or more staff members and/or members of the public have illegally undermined the business interests of the Authority for whatever purpose.
- Potential legal action arising after disciplinary action or dismissal of a member of staff.
- Illegal access to classified information from external groups acting to undermine the Authority's business interests for whatever purpose.

All staff are responsible for reporting any instances of potential or actual threats to the Authority's business interests, including fraud, to the SIRO or the Head of ICT.

5.2 Current Forensic Arrangements.

Upon receiving a report of a threat from a member of staff or from an external source, the Head of ICT will make arrangements to prevent any further access of any kind to the systems under threat.

In cases where a potential criminal investigation may result, the Head of ICT shall ensure that any systems shut down for this purpose are only brought back on line once suitable professional advice has been received and considered. The affected system(s) will only be restarted after receiving an instruction to do so from the Executive.

In all other cases, the Head of ICT will ensure that systems are brought back on line with only sufficient access rights required to conduct a review of system access and data tracking and only with the express permission of the SIRO.

The SIRO will prepare a report and any recommendations after every such incident for review by the Audit committee.

I confirm that I have read and understand my responsibilities outlined in Section 5.0: "Forensic Readiness"	*Please initial* **[MR]**

Appendix 1: Data Handling Guidance.

Portable devices (CA supplied laptops, tablets and mobile phones).

Encrypted laptop computers and tablets, as supplied by the Authority to staff, can be used to store and work upon classified information when working offline. When working remotely, any business information should be stored in accordance with the records management policy, with guidance provided by the IAO.

The device must not be used by anyone other than the employee to whom they have been assigned.

Devices must be kept in a secure place when unattended.

Removable media

All removable media must be anti-virus scanned prior to being inserted into any Authority device, in line with the ICT User Policy. CA issued iPhones must be anti-virus scanned if they have been connected to a non-Authority computer before connecting to Authority devices.

The transfer of data via USB memory stick, CD or DVD will need the permission of the IAO who will ensure that the data may be supplied. After gaining this permission, the data can be written to USB memory stick/CD/DVD by following the guidance with regards to using and encrypting removable media.

You should note that it is still permissible to copy data from USB memory stick/CD/DVD to the network or into Wisdom after appropriate anti-virus checking, in line with the ICT User Policy.

Any loss of Authority data on removable media must be reported immediately to the IAO and an information security observation should be logged immediately.

Alternatively staff many make use of the Authority's approved online file sharing system by raising a change request.

Home Computers.

The creation or storage of any business information on home computers is not allowed. Any business data held on home computers must be deleted.

Working with Third Party Organisations.

It will be the responsibility of the IAO to ensure that all external parties required to use classified Authority information (in their capacity as contractors or consultants) have been duly authorised and have signed this Information Risk

Management Policy, in addition to the Authority's Use of CA Data by Third Parties agreement form. The IAO will keep a record in Wisdom to this effect.

Data Handling.

Any requirement to provide large volumes of information to third parties other than outlined above must be with the prior agreement of the IAO who will ensure that there is a business requirement to do so and that suitable data handling agreements are in place.

The information will be copied to the media by ICT after the authorisation of a formal ICT change request has been received for this activity. ICT will provide the data in a suitably encrypted form with guidance on how the data must be handled and deleted after use by the third party.

Personal data must not be processed unless it is in full compliance with the Data Protection Act (DPA) and with the express permission of the IAO, Director and the Authority's Data Controller (Head of ICT).

Anyone needing advice or further explanation should direct their enquiries to your departmental IAO, the IA/BCP Manager, the Head of ICT, or SIRO.

Appendix 2: Government Security Classifications.

The markings to be allocated to any asset, including information, will be determined primarily by reference to the practical consequences that are likely to result from the compromise of that asset or information.

ALL information that HMG needs to collect, store, process, generate or share to deliver services and conduct government business has intrinsic value and requires an appropriate degree of protection.

EVERYONE who works with government information (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any HMG information or data that they access, irrespective of whether it is marked or not.

The three levels in the current protective marking system are OFFICIAL, SECRET and TOP SECRET and are defined below.

Currently, all information that is created, processed, generated, stored or shared within (or on behalf of) TCA is classed as OFFICIAL. If you are in any doubt or at any point you are in receipt of or are asked to handle SECRET or TOP SECRET information, then immediately contact the SIRO for guidance

OFFICIAL: Represents the majority of information that is created or processed by the public sector and as such, OFFICIAL documents do not need to be marked. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened risk profile. .

OFFICIAL - SENSITIVE: Within the OFFICIAL classification, there is some information which is especially sensitive and extra care needs to be taken in handling it. This SENSITIVE classification should only be used for information of a particularly sensitive nature and where there is a clear and justifiable requirement to reinforce the 'need to know'. The information should be marked as:

> **OFFICIAL – SENSITIVE:** with the **option** to add a descriptor to identify the sensitivity of the document as shown below:
>
> **OFFICIAL – SENSITIVE: PERSONAL**
> *(to identify sensitive information relating to an individual or group)*

OFFICIAL – SENSITIVE: COMMERCIAL
(to identify commercial or market sensitive data)

Any information marked as OFFICIAL – SENSITIVE (with or without the optional descriptors) **must** include handling requirements detailing distribution and access requirements for this sensitive information, the basic formula for which is as follows:

- **[The reason that it is classified as it is]**
- **[What you are allowed to do with this information]**
- **[What you need to do to ensure it is kept secure]**

The actual instructions will be dependent on the information to be protected. If you require any advice, contact your line manager (IAO), HoD or SIRO.

Please see the handling instructions document available from the staff Intranet for more detailed guidance and examples.

SECRET: Not applicable to TCA. Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of a serious crime.

TOP SECRET: Not applicable to TCA. HMGs most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations

More detailed Government Security Classification guidance can be found in the Risk Management section of the CA intranet.

Appendix 3: Security Classification Handling Instructions.

OFFICIAL.	
Impact.	The compromise of assets marked **OFFICIAL** may:- • Have damaging consequences if lost, stolen or published in the media. • Cause distress to individuals or a group of people. • Break undertakings to maintain the confidence of information provided by third parties. • Breach statutory restrictions on the disclosure of information. • Undermine the proper management of the public sector and its operations.
Examples.	All routine, day-to-day public sector business including policy development, service delivery, legal advice, personal data, contracts, statistics, case file and administrative data
Handling Instructions:	
Marking of all materials (paper, electronic, digital)	**There is no requirement to mark routine OFFICIAL information** (unless it is **OFFICIAL-SENSITIVE**, guidance detailed below). **Documents:** Print in bold, capitals, same size as body text, centre top and bottom of each page (header/footer). **E-mails:** Within the subject header and body of the e-mail
Storage	Physically protect by one barrier within a secure building, e.g. a locked drawer, container or filing cabinet.
Disposal of papers	Use the shredder located in the Print Room, or place in recycle bin as you consider appropriate, given the document contents.

OFFICIAL.	
Handling Instructions:	
Disposal / re-use of magnetic media	Data must not be stored, accessed or processed on any digital media not supplied by TCA. For the re-use such media, delete contents and re-use within TCA only. ICT must deal with disposal and destruction of media.
Internal distribution	Permitted in a sealed envelope.
Postage	If recipient has a "business need" to see information, mail in a sealed envelope, by post, after confirming correct full postal address including post code. **No protective marking should appear on envelopes**. Seek authorisation from IAO if moving a significant amount of information.
Discussion by telephone (landline or mobile)	No restrictions, but always confirm who you are talking to; never respond to cold caller requests for information.
Storage in WISDOM and BIW	Permitted with appropriate markings and access controls.
Email	No restrictions but should be limited to a 'need to know' basis.
Fax	No restrictions but confirm the recipient's fax number.
Photocopying	Permitted but only make as many copies as you need.
Handling Instructions:	

OFFICIAL.	
Working at home or when travelling	Permitted with the following caveats: • Laptops and removable media **must** be encrypted. • Information must not be e-mailed to or from home e-mail accounts, or held in personal data stores. • Papers/portable media to be kept out of sight. • Care must be taken to ensure that information cannot be inadvertently overlooked.

Key:

Allowed	Allowed with caution

OFFICIAL – SENSITIVE.	
Impact.	In addition to the impacts listed for OFFICIAL in the table above, the compromise of assets marked OFFICIAL – SENSITIVE would be likely to cause a greater level of damage or distress due to the sensitive nature of the information.
Examples.	Our most sensitive corporate or operational information, policy development and advice to ministers on contentious/very sensitive areas. • Sensitive personal data, such as medical records and salary information. • Information about investigations and civil or criminal proceedings that could prejudice court cases. • Security information such as security reports and vulnerabilities

OFFICIAL – SENSITIVE.	
Handling:	
Marking	**Documents:** Print in bold capitals, same size as body text, centre top and bottom of each page (header/footer) **E-mails:** Within the subject header and body of the e-mail. Add a Descriptor if appropriate, which must be either '**COMMERCIAL**' or '**PERSONAL**' Handling requirements **must** be included in the body of either the document or the e-mail detailing the distribution and access restrictions. • See GSC Handling Instructions for examples.
Storage	Physically protect by one barrier within a secure building, e.g. a locked drawer, container or filing cabinet.
Disposal of papers	Dispose with care - use the shredder located in the Print Room.
Disposal/re-use of magnetic media	Delete contents and re-use within CA only. ICT must deal with disposal and destruction.
Internal distribution	To recipient by email, sealed envelope, through internal post, or deliver by hand. When moving assets by hand or internal post, follow OFFICIAL handling instructions **in addition to** using a nondescript container/envelope - write the classification on the inner envelope only.

OFFICIAL – SENSITIVE.	
Handling:	
Postage	Use a single, unused envelope (with no classification marking) and include return address on the back of the envelope. Consider using a double envelope and writing the classification on the inner envelope only. Consider using Royal Mail next day tracked delivery service or a reputable commercial courier's 'track and trace' service. Confirm the recipient's full postal address including post code before despatch.
Discussion by telephone or video conference	No restrictions, but always confirm who you are talking to and keep details to a minimum. Note that telephony systems should not be assumed to be secure. Details of sensitive material should be kept to an absolute minimum.
Storage in WISDOM	Permitted with appropriate markings and access controls
Email	Information **must** be encrypted if sending externally using 7-ZIP or WinZip. Information may be sent unencrypted internally, but you should assess the risk of it being intercepted and exposed. Consider whether the e-mail could be forwarded on outside of TCA and, if so, it should be encrypted.

OFFICIAL – SENSITIVE.	
Handling:	
Fax	Keep information to be faxed to a minimum. Confirm the recipient's fax number. Ensure recipient is waiting to receive the fax.
Photocopying	Permitted but only make as many copies as you need and control their circulation.
Working at home or when travelling	In addition to those conditions for OFFICIAL , the following apply when dealing with **OFFICIAL – SENSITIVE** information: • Information should not be opened or worked on whilst travelling or in public areas. • Papers/laptops/portable media must never be left unattended. If working from home, papers must be stored in a locked drawer/cabinet.

Key:

Allowed	Allowed with caution

Appendix 4: Information Risk Management – WISDOM.

WISDOM Security Classifications.

Following consultation with Directors and Line Managers, security classifications have been applied to the system. Wisdom is configured so that classifications applied in the file plan at class and folder level are cascaded to documents registered into those folders.

How to create and handle OFFICIAL information in Wisdom is explained below.

WISDOM Responsibilities.

IAO's (Line Managers):

Responsible for defining the records classifications within their own business area and agreeing them with their Director and HoD. Line Managers must ensure that their staff understand and comply with the requirements for records classification.

WISDOM Departmental Records Administrators (DRAs):

Responsible for maintaining the file plan for their business area. New security classification settings should only be applied following discussion and agreement with Line Managers.

WISDOM Users:

All staff are responsible for registering business related documents and records into the Wisdom file plan in accordance with the Handling and Security of Paper and Electronic Records Policy, with the appropriate security classification applied by the DRA. Any issues should, in the first instance, be raised with the DRA who in turn will resolve with the Line Manager/IAO.

Appendix 5: Sign Off Sheet

This sign off sheet relates to the Coal Authority Information Risk Management Policy.

- Should you have any enquiries, please contact Paul Frammingham (SIRO) on extension 386 (01623 637386).
- This form **must** be signed and returned to the Coal Authority HR Department or the Coal Authority manager who sent it to you (for external consultants).
- You should keep a copy of the form and policy for your own records.

I acknowledge receipt of and agree to comply with the document entitled: 'Information Risk Management Policy'

Signature……Date……03/12/2019……

Print Name (block capitals please)

MYLENE RECEVEUR……..

Policy Documentation:
Information Risk Management (IRM) Policy.

DOCUMENT CONTROL:

Document Title: Information Risk Management Policy 310513

Current Version: v3.3

Author/ Owner: Paul Frammingham

Wisdom Ref: 003226121 (CA00/16/1)

Approved By:

Name	Role/Responsibility	Date
Paul Frammingham	Director of Finance & Corporate Services (SIRO)	12 Sep 2016

Reviewed By:

Name	Role/Responsibility	Date
Matthew Thorpe	Head of ICT	12 Sep 2016
Dan Whitt	Senior ICT Manager	12 Sep 2016

Document Authors:

Name	Role/Responsibility	Date
Ragnar Karlsson	Information Assurance & Business Continuity Manager	12 Sep 2016

Change History:

Author(s)	Change Commentary	Version	Date
Ragnar Karlsson	Final version agreed for sign-off by	3.3	12 Sep 2016

Author(s)	Change Commentary	Version	Date
	Audit Committee		
Ragnar Karlsson	Minor edits to ensure currency.	3.2	18 Jul 2016
Ragnar Karlsson	Updated to refresh current training requirements and add include links to risk management and disciplinary actions	3.1	20 May 2016
Dan Whitt	Circulated for Audit Committee review of currency and signoff	3.0	10 Aug 2015
Dan Whitt	Updated version circulated for Audit Committee signoff	3.0	09 Apr 2014
Dan Whitt, Anita Jones	Updated in line with revised government security classifications effective 2nd April 2014	2.1	24 Mar 2014
Dan Whitt	2013 revisions and stakeholder feedback incorporated.	2.0	04 Jun 2013
Dan Whitt	2013 revisions and stakeholder and Audit Committee review.	1.1	03 Jun 2013
Steve Pennell	Final document version sign off.	1.0	01 Sep 2011