

Department of the Interior  
<Bureau>  
<Office/Organization>  
Emergency Response Center

## Information Management Awareness and Best Practices

The Department of the Interior (DOI) has a legal requirement to protect the information it collects and maintains on employees and the public, to preserve and manage the Federal records in its custody, and promote transparency in our government operations. In keeping with these requirements, the Department has put in place a set of rigorous policies and procedures for employees to follow to ensure compliance in the information management activities related to Privacy, the Freedom of Information Act, and Records Management. It takes both management support and employee cooperation for DOI to successfully meet its information management obligations. Failure to follow these requirements may lead to disciplinary action up to and potentially including removal, and could also be the basis for lawsuits and civil or criminal penalties; therefore it is of the utmost importance that all DOI employees understand their information management responsibilities.

### **Records Management**

- Recognize the importance of agency records. A record is any item, in any physical form (paper, email, electronic file, CD, voice clip, video clip, etc.) that advances or represents agency work, including any small step in that process. The Federal Records Act requires agencies to preserve and protect records, to manage them in an organized, retrievable manner, and to create and implement filing and scheduling plans for their final disposition.
- Each bureau has a Records Officer, and many offices also have a Records Contact, to assist with any records management matters for the bureau. Please reach out to your bureau's records officer with any questions regarding records management activities (<http://www.doi.gov/ocio/records/people/recon.htm>).
- Identify and protect all records currently associated with a preservation or litigation hold, such as the Deepwater Horizon BP oil spill, Tribal or Indian Trust records. Your supervisor will identify any categories of such records and provide additional guidance.
- Save as an official record all information in any form (email, paper, electronic files, photographs, etc.) that record agency functions, decisions and actions taken as part of your work at DOI.
- Keep official documents filed properly and in a logical manner for efficient retrieval, and be sure to keep official documents separated from personal documents.
- Assist your office's records contact with any requests concerning records for which you have any activity or control.
- Document any work activities (such as making a note of a phone call affecting agency operations).

- Do not remove or allow records in your care to be removed from agency custody unless explicitly authorized by your supervisor.
- Ensure the appropriate levels of safeguards are implemented to protect records in your possession, especially records that contain sensitive information.
- Do not destroy or alter existing records without explicit authorization from your supervisor.
- If any records are being moved pursuant to a chain of custody process, make sure to follow each step to the letter, and do not allow unauthorized access to agency records.
- If issued a mobile device (e.g., laptop, BlackBerry, etc.) keep it secure at all times, and out of sight or in a completely secure location when not in use. Also ensure mobile devices are encrypted and password protection is enabled.
- Report any problems immediately to your supervisor or bureau Records Officer.
- Additional records management information is available at <http://www.doi.gov/ocio/records/index.html>.

## Privacy

- Recognize privacy information. Privacy information is any information that identifies or describes an individual. Examples of privacy information include, but are not limited to, Social Security Number, family information, financial information (including credit card numbers, banking information and credit score), medical information (including illness, medicine, or disability), legal or criminal history, personal contact information such as home address, personal phone number, personal email address, biometric information including photos and fingerprints, non-work memberships and affiliations, etc.
- Each bureau has a Privacy Officer who will provide expertise on privacy matters. Do not hesitate to contact these individuals with any questions regarding the management of privacy information ([http://www.doi.gov/ocio/privacy/doi\\_privacy\\_act\\_officers.htm](http://www.doi.gov/ocio/privacy/doi_privacy_act_officers.htm)). If you have a legitimate reason to share privacy information at work, such as transmitting it to a payroll office for payment, fax it to an attended fax machine and ensure that someone is there to pick it up immediately, and confirm receipt from the receiving office.
- If you receive an e-mail that contains privacy information that does not belong to you in the subject, body or attachment(s) of the message, DO NOT forward it to anyone. Ensure the recipient of any privacy information has an official need to know (contact your DOI supervisor for further guidance).
- Refer all requests for privacy information or access to privacy records to your supervisor. These requests are processed through the Bureau FOIA Office.
- Maintain the complete confidentiality of any privacy information you have access to as part of your work at DOI. Do not email privacy information from the DOI network unless encrypted. This includes Social Security Numbers, credit card numbers, passwords, or any other information about individuals (including you). Doing so violates DOI policy as stated in the DOI Security Policy Handbook, Version 3.
- Do not send any privacy information to your personal email address in order to work at home; this violates DOI policy as information transferred outside of the DOI network may not be encrypted or secure.

- Do not share your password with anyone for any reason as it may be used to access the DOI network and restricted privacy information.
- Keep official items such as a badge, keys, laptops, mobile phones, documents, CDs, etc. completely secure at all times, and ensure unauthorized personnel do not gain access to them. Report the loss of these items immediately to your supervisor as they may contain privacy information or be used to gain access to restricted information or agency areas.
- When you are not present, secure your computer and any paper documents with privacy information. When working, ensure privacy information is not visible to visitors.
- Use the official DOI Privacy Act Warning Notice on files and filing cabinets to protect records that contain privacy information, see [http://www.mydoi.doi.net/ocio/imd/ocio\\_privacy\\_guidelines.html](http://www.mydoi.doi.net/ocio/imd/ocio_privacy_guidelines.html).
- When speaking at work, whether in person or on the telephone, ensure that third parties cannot overhear any privacy information discussed.
- Report any suspected loss or compromise of privacy information **IMMEDIATELY** to your supervisor. DOI must report suspected privacy breaches to U.S. CERT within **1 hour** of discovery.
- If in doubt about how to handle any privacy information or issue, discuss it with your supervisor or your bureau Privacy Officer.
- Additional privacy information is available at <http://www.doi.gov/ocio/privacy/>.

### **Freedom of Information Act (FOIA)**

- The Freedom of Information Act (FOIA) is a law that allows individuals to request records from the Department. The Department releases records unless they are protected by a FOIA exemption. The FOIA exemptions protect information in Department records, such as privacy, commercial, financial, law enforcement, and other sensitive information.
- Each bureau has a FOIA Officer to handle such requests and respond on the bureau's behalf (<http://www.doi.gov/foia/contacts.html>).
- Do not release any Agency records. Refer all requests for information/records to your DOI supervisor for follow up action with the Bureau FOIA officer.
- The FOIA exemptions protect information in Department records, such as privacy, commercial/financial, law enforcement, and other sensitive information.
- Be sure to cooperate with any request for a documents search from DOI FOIA personnel; they are under tight statutory deadlines and have a legal mandate to comply.
- Further FOIA information is available at <http://www.doi.gov/foia>.

### **Conclusion**

We welcome you to the DOI work force and want your term of employment to be a successful one. It is important that you understand your information management responsibilities and incorporate these best practices into your work activities to ensure DOI successfully meets its legal obligations to protect and manage privacy information and agency records. We appreciate your assistance and support.