



United States Department of the Interior
BUREAU OF LAND MANAGEMENT
Oregon State Office
P.O. Box 2965
Portland, Oregon 97208



In Reply Refer to:
1260/1278/1283 (OR955) P

February 11, 2011

EMS TRANSMISSION 02/15/2011
Instruction Memorandum No. OR-2011-024
Expires: 9/30/2012

To: All Oregon/Washington Employees
From: State Director, Oregon/Washington
Subject: Management of Backup and Storage of Electronic Data and Files

Program Area: Information Resources.

Purpose: Establish the policies and procedures to guide the backup and storage of electronic data and files in Oregon/Washington (OR/WA).

Policy/Action: It is every employee's responsibility to ensure that all data and files that have a continuing value to the Bureau of Land Management (BLM) are stored on a corporate drive so they can be backed up on a regular basis. Attachment 1 contains information about the backup procedures, retention of each type of backup, and retrieval of data or files from the backups.

Online storage of data and files can incur significant costs if not managed properly. Each employee is to review files in his/her corporate directories that have not been accessed in the last two years and determine whether they should continue to be kept online. Work with your local records manager if you need help determining whether files that are not needed are considered records. Any non-record files/data that are not needed should be deleted. Data that is deemed a record cannot be deleted due to ongoing litigation that prohibits the deletion or destruction of any BLM records.

Data is to be stored on government-issued equipment and placed in appropriate areas. If the data is sensitive (e.g., personally identifiable information, data not releasable under the Freedom of Information Act), it should not be stored on removable storage devices (such as memory cards, universal serial bus thumb drives, portable hard drives) unless the device can be encrypted and is password protected.

No personal data (music, video, games, pictures, documents, photographs) are to be stored on government computers.

Photographs are an important part of how we manage the public lands. However, when unmanaged, they can easily get out of control and use significant amounts of storage space. Employees that take and store photographs need to review their photographs on a regular basis and delete any duplicates or those no longer needed. Also, most photographs are taken and stored at a much higher resolution (megapixels) than is needed for their intended purpose. There is software on all employees' workstations (Microsoft Office Picture Manager) that can be used to reduce the file size of these photographs without losing picture quality (800 x 600 is adequate for most purposes). See Attachment 2 for instructions on adjusting a photograph's size.

All imagery data is to be managed by the OR/WA Branch of Information Resources Management. This includes (but is not limited to) satellite images, aerial photography, digital raster graphics, digital orthophoto quads, scanned maps, and Light Detection and Ranging data and derivatives. Management of the data includes backups, storage, and providing imagery through online locations as well as the use of sites outside of OR/WA BLM, such as the United States Forest Service's Remote Sensing Applications Center image server or the BLM National Operations Center image server.

Timeframe: Effective immediately.

Budget Impact: As electronic files grow in number and size, the cost of backup and online storage will grow. This policy will control associated costs and maintain them at an acceptable level. Deleting non-record data from corporate drives not only results in more space available for ongoing work, but also reduces the need to purchase additional storage devices and backup media and lowers off-site storage costs.

Background: The storage and backup of data and files is becoming a significant issue as the BLM's holdings of electronic information expand. Just as with other agencies and companies, electronic data and files stored on corporate drives is growing at a rapid pace. This policy is intended to provide a structure to how OR/WA BLM manages this growth. Budgetary limitations make it imperative that these costs be controlled while maintaining ready availability to the data and information needed for ongoing work.

Manual/Handbook Sections Affected: None.

Coordination: Records Management, Data Administration, Information Technology Management and Operations, and ad hoc committee with representatives from Division of Resource Planning, Use, and Protection (OR930), Division of Management Services (OR950), and five districts.

Contact: Stanley Frazier, Directory Structure Project Manager/State Data Administrator, 503-808-6009.

Districts with Unions are reminded to notify their unions of this instruction memorandum and satisfy any bargaining obligations before implementation. Your servicing Human Resources Office or Labor Relations Specialist can provide you with assistance in this matter.

Signed by
Michael Mottice
Associate State Director

Authenticated by
Rita Wallberg
Records Section

Attachments

- 1 – Data Backup and Storage (4 pp)
- 2 – Photograph Size Adjustment (2 pp)

Distribution

WO500

DATA BACKUP AND STORAGE

This attachment contains definitions related to data and file backup and storage, roles and responsibilities, and information about the backup schedule, how long data is retained, and procedures to recover or restore data from a backup. Also included is a list of references to policies, standard operating procedures, and related documents that have bearing on this topic.

Definitions

Archive – A copy of data that is made for preservation purposes. Some archives may be regularly scheduled, but most are not. Archives are business-driven and are less accessible than backups. Archives cannot be changed and are kept permanently. Archives are transferred to a Federal Records Center (FRC) and eventually to the National Archives and Records Administration (NARA).

Backup – A copy of data that is made for restore/recovery purposes. Backups are regularly scheduled. Backups are information technology-driven and may be kept in a variety of locations (near storage, offline, off-site). Backups are only kept temporarily (although temporary may mean for a year or longer).

Reference Data – Data that has a continuing value to the business, usually at the completion of a project, and is kept online even though the rest of the associated data is moved off-line.

Records – The basic definition is found in the Federal Records Act. Records are defined as “all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government” [44 U.S. Code, Chapter 33, Section 3301] and needed to document agency activities or actions.

Sensitive Information – Information or data that requires protection due to the risk and magnitude of loss or harm which would result from inadvertent or deliberate disclosure, alteration, or destruction. The term includes information or data the improper use or disclosure of which could adversely affect the ability of the agency to accomplish its mission, privileged data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act.

Roles and Responsibilities

System Administrators – Physically perform backups on set schedules using Standard Operating Procedures (SOPs). Create archives when directed to do so by the State Records Administrator, State Data Administration, or State Data Stewards using SOPs.

Records Administration Staff – Work with data stewards and others to identify proper records retention schedule for data, identifying which data are considered records and which records need to be formally archived.

Data Administration Staff (primarily at the State Office) – Work with Information Technology staff/system (OR955) administrators to assure that backups are performed as required and managed properly. Work with Records staff to properly define records retention and archive requirement in data standards and other data documentation.

Managers/Supervisors – Work with employees that are leaving government service to assure that any data (including email) is available for use by other employees. Allow data stewards sufficient time to perform their duties related to archiving and backups.

Data Stewards – Work with Records staff to properly assign retention to data for which they are responsible. Understand Backup and Archive policy and assure that data is properly managed under those policies.

Employees – Work with local records manager on disposition of data when no longer needed. Work with their supervisors to relocate their data (including email) for use by other employees before leaving government service.

Backup Frequency

Backups are made on a regular schedule as defined by the SOPs and Service Level Agreements between OR955 and Oregon/Washington Executive Managers (District Managers, Deputy State Directors). In general, backups are performed each work night and at the end of each week. Backups are copied to tape and sent to off-site storage on a monthly, quarterly, and annual basis. Files and data on non-Microsoft Windows servers (email, UNIX) are backed up directly to tape and sent to off-site storage.

Backup Retention

Most backups are not kept on a long-term basis however the current prohibition on destruction of records (as a result of various lawsuits) places an “Infinite” retention on the yearly backup tapes. All email tapes also have a permanent retention.

What is Backed Up

All network user and share drives (both in the State Office and in the Field Offices) are currently backed up. This includes data storage locations accessed by the Citrix servers with one exception noted below. Email and other non-windows server-housed data are also backed up.

What is NOT Backed Up

Local workstation drives (C:/, D:/, etc) **are not** backed up. There is also a 50 gigabyte partition of the servers in the District Offices (used for local data, primarily geographic information system) that is not backed up. No backups are performed on the Citrix-managed I:/ drive (Imagery). The imagery drive only contains copies of static data thus not requiring any backups.

Removable storage devices such as portable hard drives or universal serial bus (thumb) drives are not backed up.

Removing Electronic Data/Files

Non-record material may be removed (deleted) when no longer needed. Removal of this material will reduce the amount that is required to be included in each of these backups.

Retrieval of Files/Data

The retrieval and restoring of data and files from backups are initiated by placing a Help Desk request (through Lotus Notes, 1-800-BLMHELP, or <http://1800blmhelp.blm.gov/index.php>). The length of time it takes to actually restore files from a backup is dependent on the type of backup that is being restored. Files contained on the online backup locations can be retrieved fairly quickly. Requests for restores from backups that are contained on tape and are off-site may take a week or more.

Things to Remember

The longer a file has been on a backup tape, the less likely it can be retrieved. Currently the State Office has tapes that go back to 2005 (and some further than that) but tapes deteriorate over time and software and hardware incompatibilities become an issue.

If you decided that you no longer needed some non-record files and deleted them, they may or may not exist in the backups. Backups are a means to restore files accidentally lost or deleted and should not be relied upon as a “fail-safe” system.

Anything that is a “record” cannot be deleted and anything that is a “permanent record” must be archived to the FRC/NARA. Consult with your local records manager on this issue.

References/Authorities

[OR-SOP-053-001](#): Restore From SnapShot Backup Procedures

[OR-SOP-071-000](#): Tape Backup Restore Procedure

[OR-SOP-051-000](#): Tape Librarian

Information Bulletin [OR-2008-089](#): Employee Responsibilities for Electronic Data

Instruction Memorandum [OR-2009-034](#): Management of Digital Information and Data

Instruction Memorandum [OR-2009-051](#): Data Management Roles and Responsibilities

[36 U.S. Code, Chapter 12, Subpart B](#): Records Management

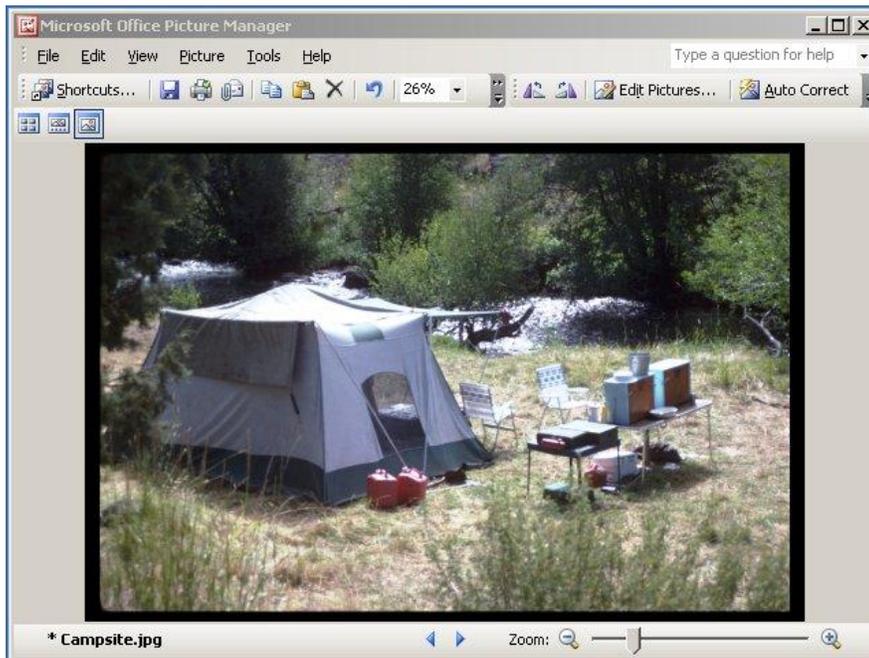
[44 U.S. Code, Chapter 33](#), Section 3301: Definition of a “record”.

[BLM Manual 1278](#), External Access to BLM Information

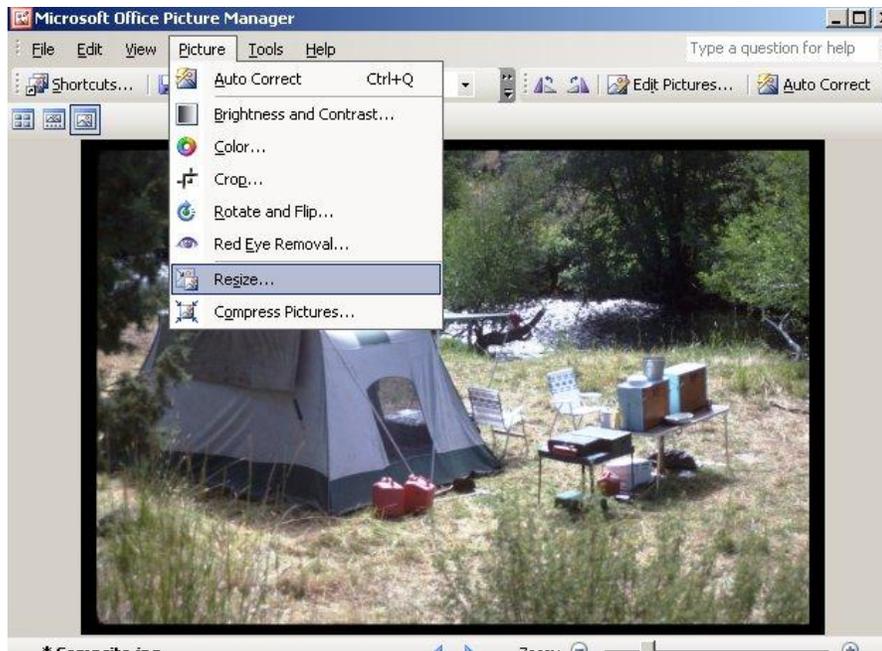
PHOTOGRAPH SIZE ADJUSTMENT

Most photographs taken with digital cameras or scanned are much larger in file size and resolution than is necessary for computer screens and printers. This makes the file size of our documents too big for rapid downloading and display, especially when dealing with remote servers such as SharePoint (in Denver) or Citrix (in Portland). Here are a few steps to modify your photographs so that they look great while still maintaining a small file size:

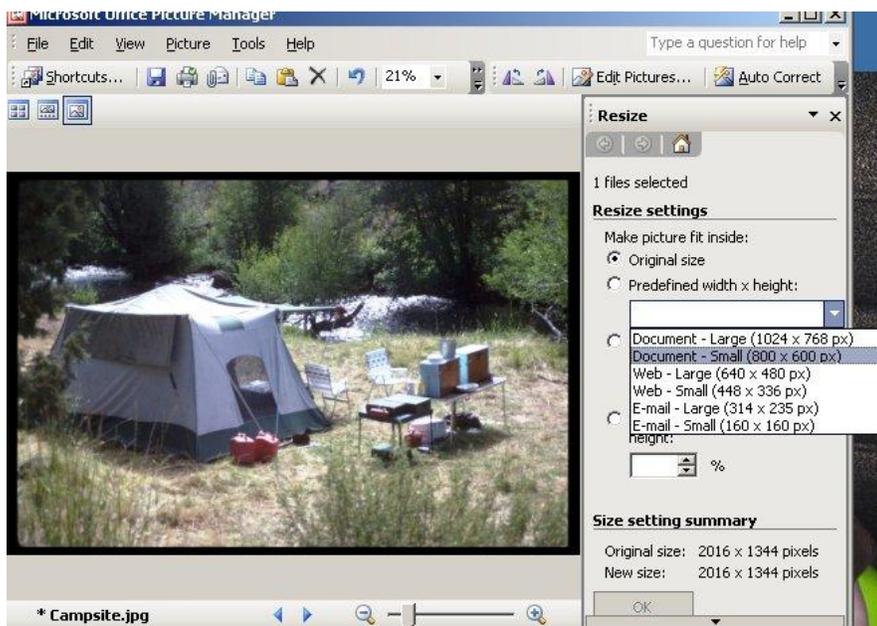
1. Navigate to the folder where your pictures are located.
2. Find a photograph that you want to modify due to its size (anything over 500 KB).
3. Right click the file name and select "Open with" and choose Microsoft Office Picture Manager. This program is part of Microsoft Office and is available on any Bureau of Land Management workstation. If the Picture Manager program does not appear on the initial drop-down list, click Change Program and select Microsoft Office Picture Manager, and click OK.



4. Click the "Auto Correct" button in the upper right portion of the menu. This almost always improves the color, contrast, hue, and brightness.
5. Click the "Picture" menu and select "Resize."



6. Choose "Document Small" (800 x 600 px) from the "Resize Settings Menu." You can also choose a smaller resolution (640 x 480 px or less).



7. Click the "OK" button on the bottom of the Resize panel and then save the file (Ctrl-S or File > Save).

Always "insert" graphic files into your programs instead of pasting them. This allows the program to adjust the image more efficiently. When you *insert* your graphic file into a document, it may be smaller than you'd like. Just use that program's features for stretching/resizing the program. This way, the original file size stays the same.