P.O. Box 2890
Washington, D.C.
20013

1. Purpose:

To provide NRCS employees and partners the Standard Operating Procedures (SOP) for encryption and password protection to safeguard sensitive and private information through the use of WinZip (archive utility for Windows).

2. Scope:

This SOP will be used by all employees and partners to transmit sensitive and private information through Microsoft (MS) Office Outlook.

3. Outline of Procedure:

4.1 Definitions
4.2 Roles and Responsibilities
4.3 How to Use WinZip for Encryption with password protection.
4.4 Rename the WinZip file for transmission through MS Office Outlook.
4.5 Correct method for the transmission of the WinZipped file and the password through MS Outlook.

4. Specific Procedures:

4.1 Definitions

A. WinZip:
WinZip, the archive utility for Windows, is an easy-to-use, time saving tool that reduces the size of files and provides password-based AES encryption to protect confidential information.

B. Sensitive and Private Information:
Per GAO: "…Sensitive data, including personnel, customer accounts, and financial information…"

"…Sensitive data—including information relating to the privacy of U.S. citizens, payroll and financial transactions, proprietary information, agricultural production and marketing estimates, and other mission critical data…"

THE PRIVACY ACT OF 1974: "…establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to

Helping People Help the Land
An Equal Opportunity Provider and Employer

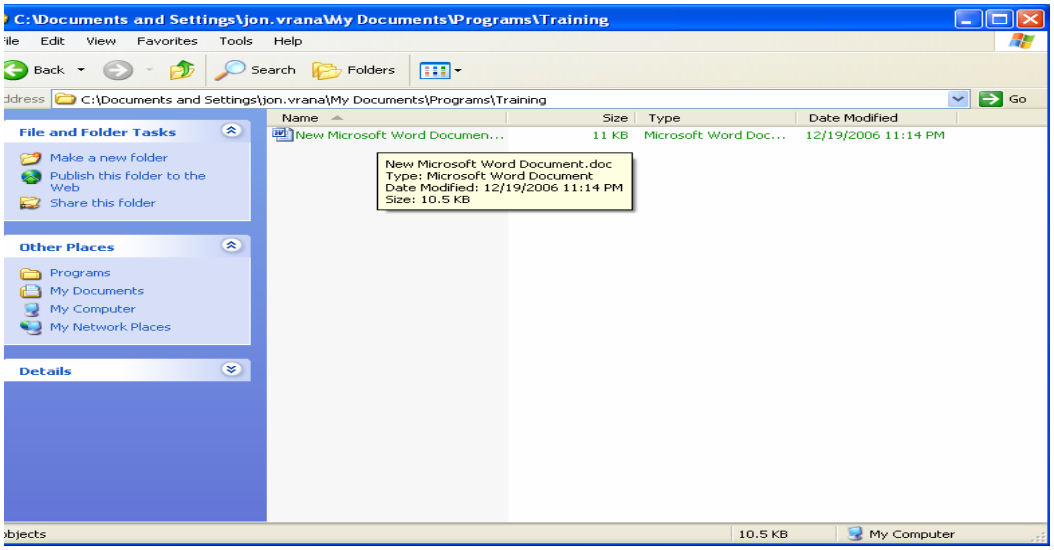
protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained…"

4.2 Roles and Responsibilities

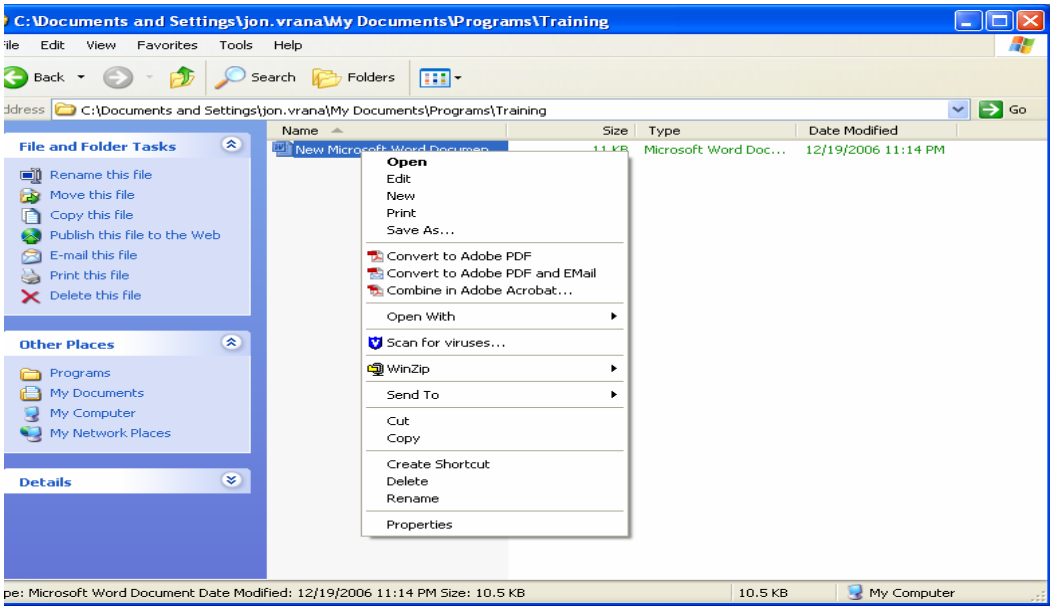
A. Employees and Partners:
All permanent employees, temporary employees working over 30 days, contractors, volunteers, and partners, including Conservation District and RC&D employees, who have access to NRCS computer systems, networks, and email are responsible for ensuring the protection of transmitted private and sensitive information.

4.3 How to use WinZip for Encryption with password protection

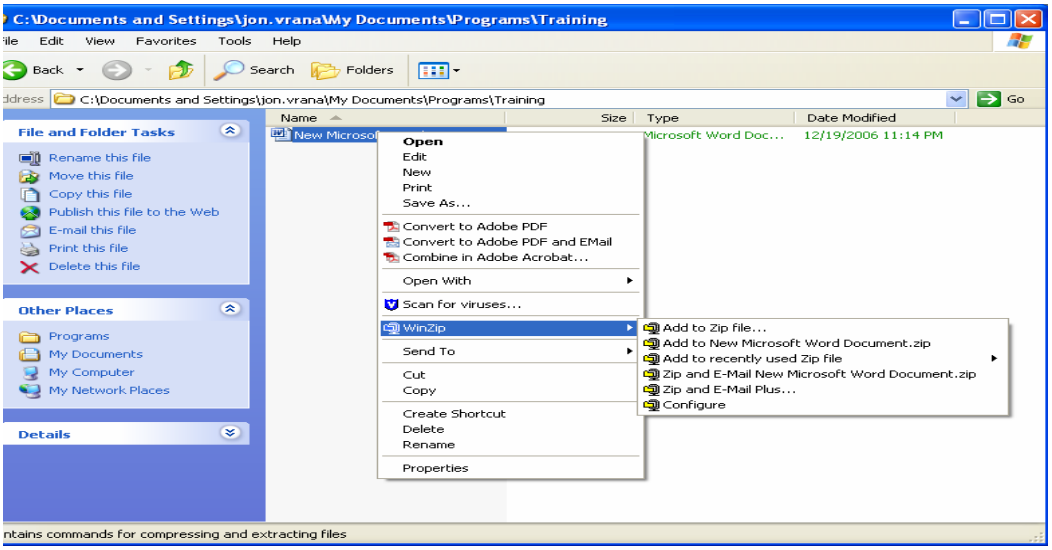
4.3.1 Locate the document that you need to zip, using Windows Explorer.



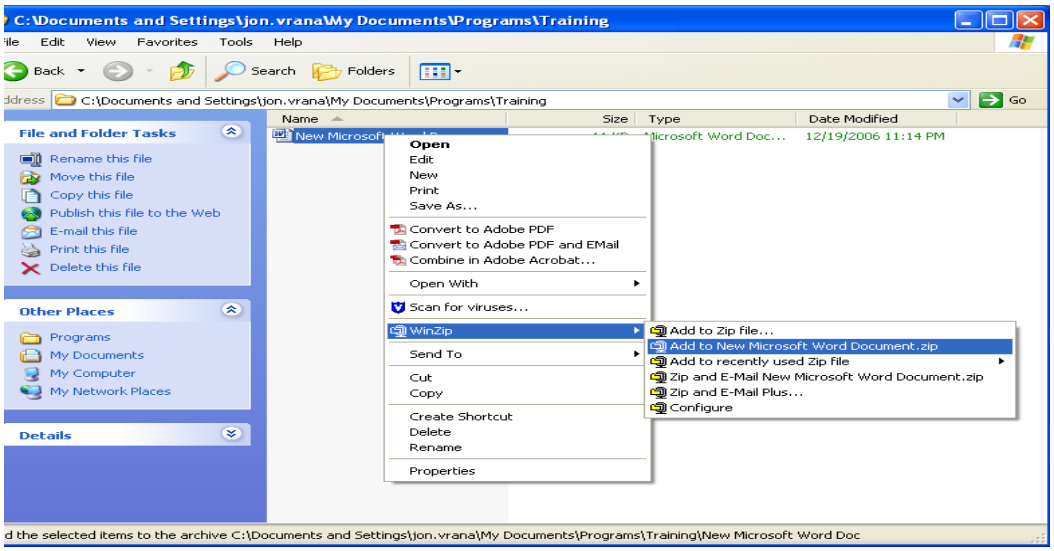
4.3.2 Right mouse click on the file to bring up the menu containing WinZip.



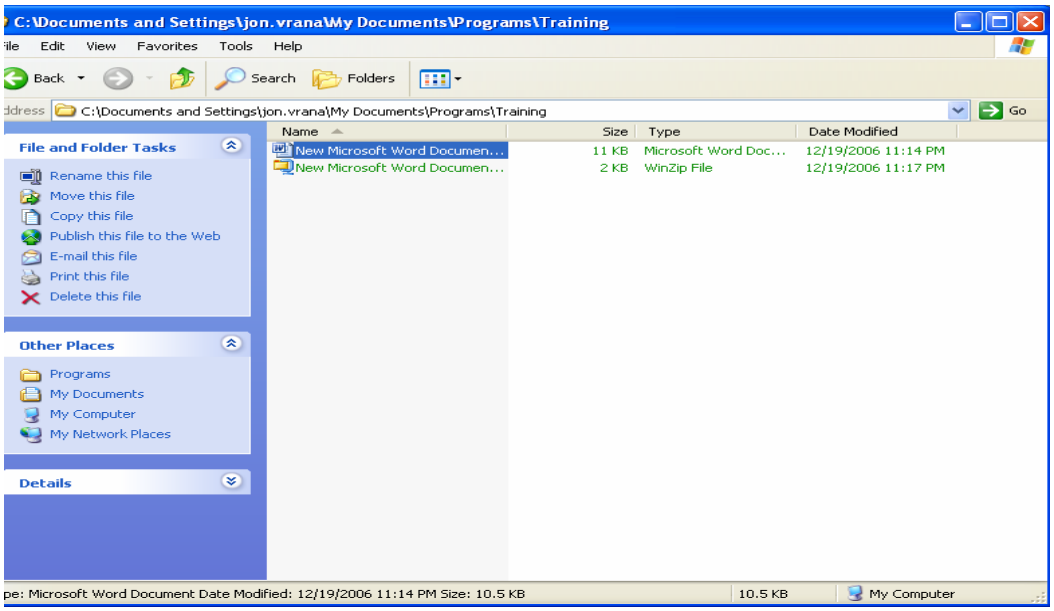
4.3.3 Highlight WinZip on the menu to bring up the WinZip submenu.



4.3.4 Select the second option “Add to *FileName*.zip.” Once you select this option, the file will automatically be zipped and the zipped file placed in the same directory as the original file.

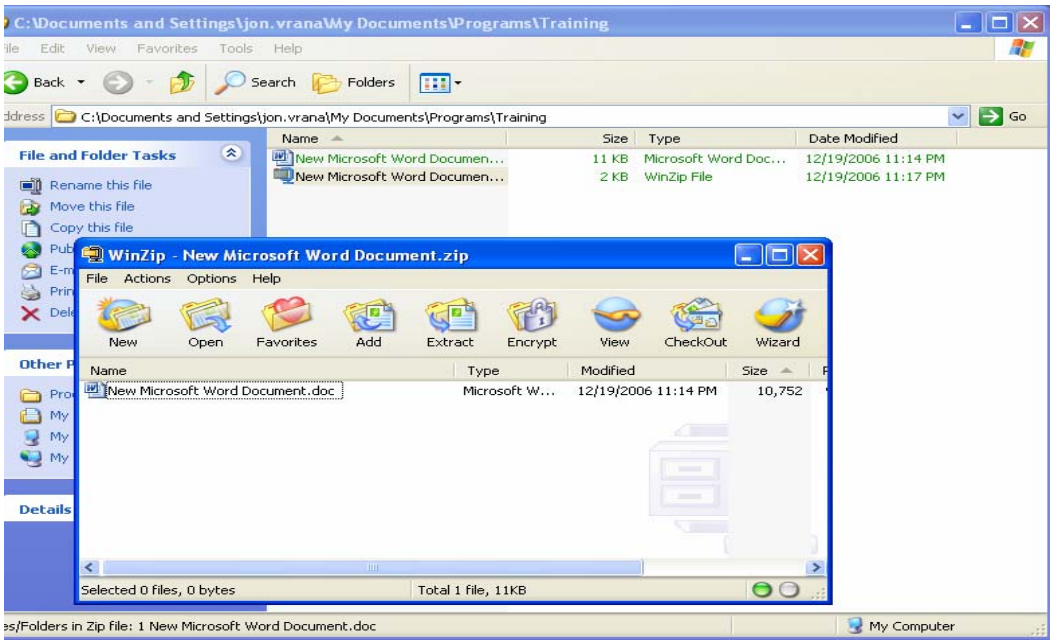


4.3.5 Here you can see the original and newly created WinZipped versions of the file.

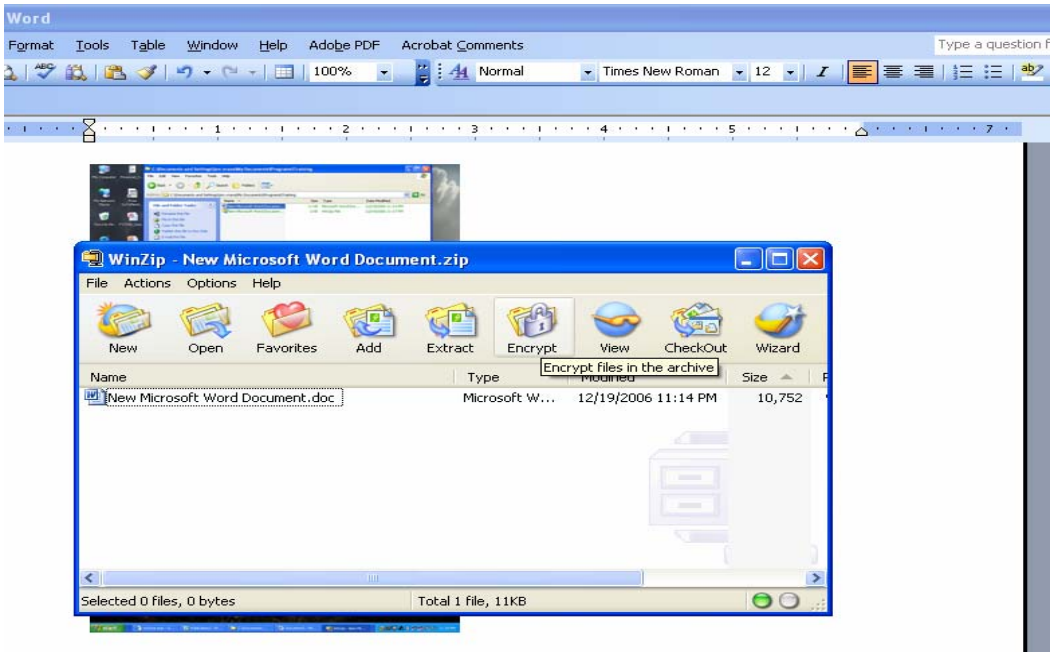


4.3.6 Double-click on the zipped file to open up the WinZip dialogue screen. The dialogue

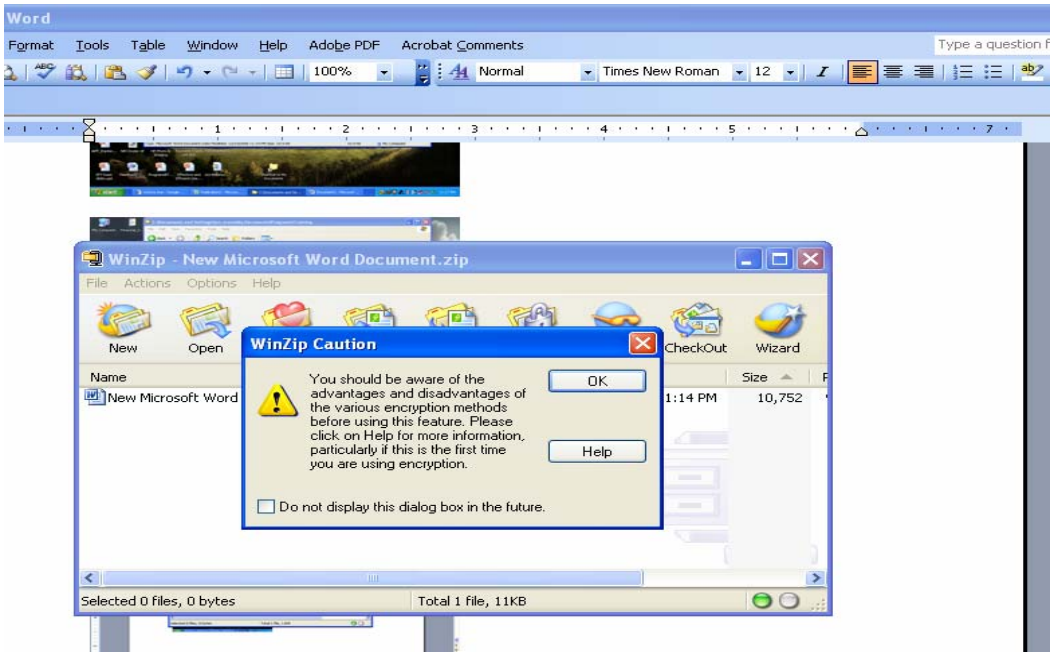
screen will display your original file.



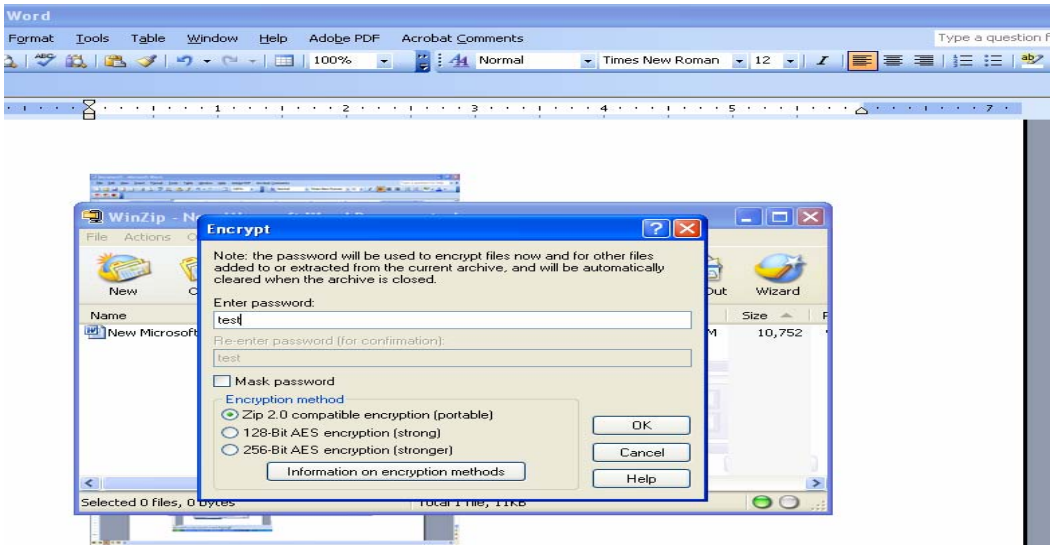
4.3.7 Click on the “Encrypt” button on the WinZip tool icon bar to begin the password protection process.



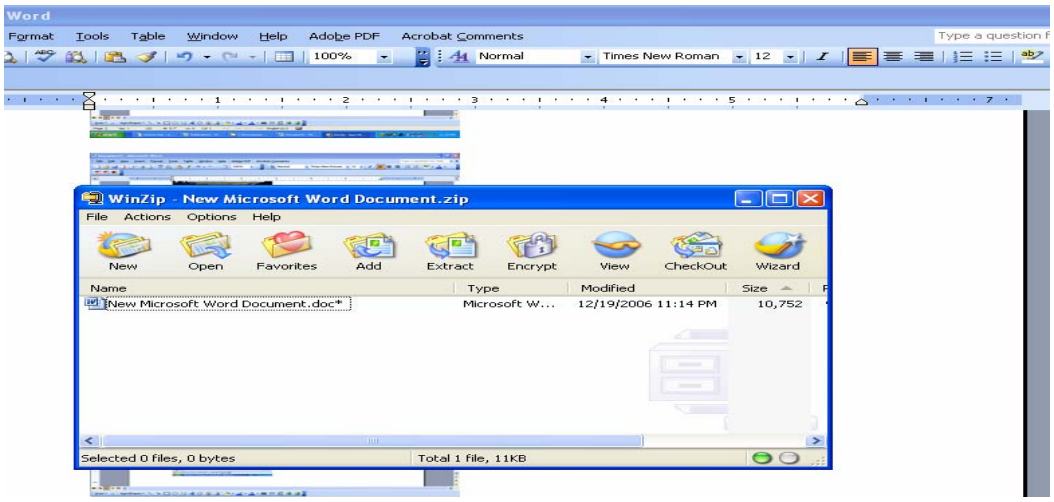
4.3.8 Initially, a caution box will pop up, but ignore it and click “OK.”



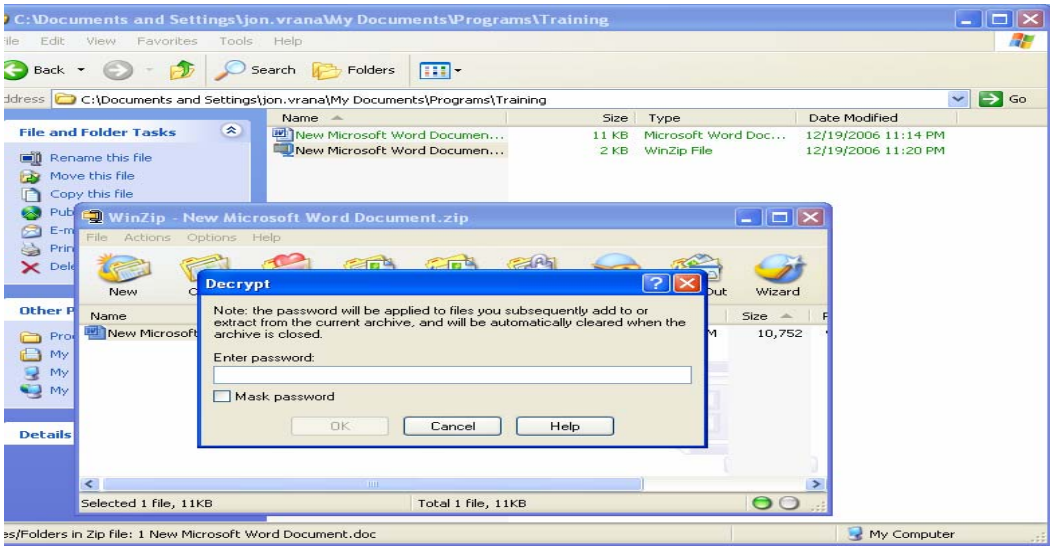
4.3.9 Enter a password in the next pop-up window. Change the encryption type to "256-Bit." It's the strongest. Click "OK." The file is now WinZipped and password protected. **NOTE: The file displays an "Asterisk (*)" at the end, denoting an encrypted file.**



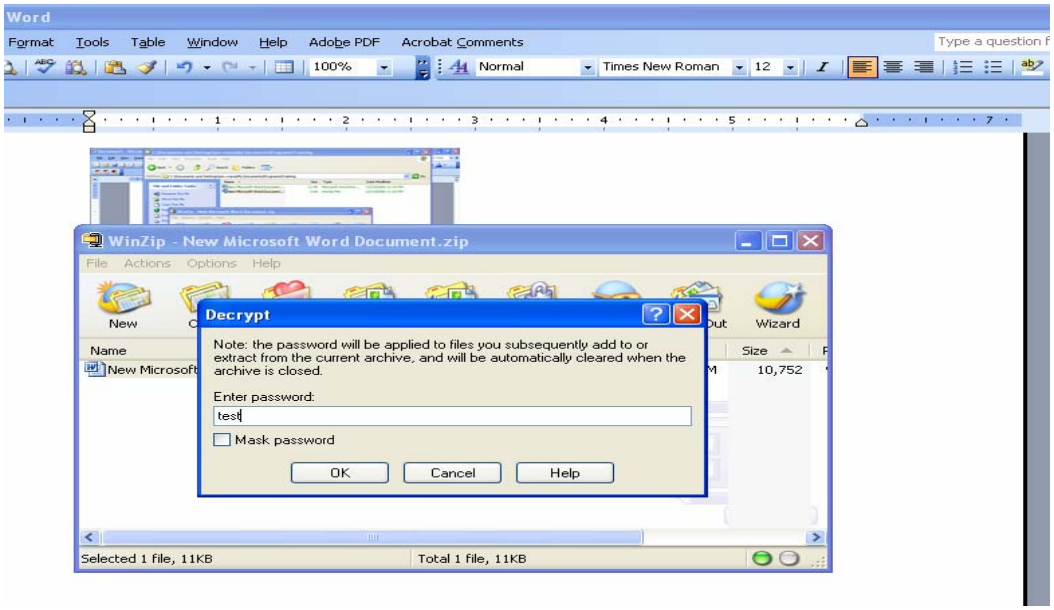
4.3.10 To test the password protection and WinZip process or to open a previously WinZipped and password protected file; double-click on the WinZipped file. The WinZip pop-up window will be displayed as shown below.



4.3.11 Double-click on the asterisk denoted file and a window will pop-up that requires you to enter a password.



4.3.12 Enter the required password, leave all other enter items as defaulted, and click on "OK." The file will be automatically opened in the appropriate Microsoft product (e.g. Word, Excel, PowerPoint, Access). Select File->Save As to save the file in the appropriate directory.



4.4 Rename the WinZip file for transmission through MS Office Outlook

Per OCIO-ITS Customer Service Alert, dated April 13, 2007, "…the Service Center Agency (SCA) network continued to see infections caused by the virus variants… a proactive measure of sweeping through unopened/unarchived messages in user's inboxes for *.zip files is currently underway. Wildcard variants of *.zip files (such as .zap or .zop) will also be deleted. If found, these zip files will be deleted. While this will cause some legitimate business impacts, this action increases the success of removing this infection quickly. As*.zip files are deleted, they will also now be blocked by the perimeter Exchange equipment, and will no longer pass from sender to receiver within the SCA environment. If legitimate *zip files need to be sent to pass under the size limitations of Email, user's must rename these files to exclude the *.zip extension."

4.5 Correct method for the transmission of the WinZipped file and the password through MS Outlook.

The password must be sent in a separate email to the receiver than the e-mail containing the WinZipped file.

5. Technical Contact:

1/22/08

Approved By: JACK R. CARLSON Date
Chief Information Officer

USDA, NRCS
1400 Independence Avenue, S.W.
Room 6218-S
Washington, D.C. 20250
(202) 690-0242

1/22/08

Approved By: DENNIS J. LYTLE Date
Operations Branch Chief

USDA, NRCS
2150 Centre Avenue, Building A
Fort Collins, CO 80526-8121
(970) 295-5485