



United States Department of Agriculture  
Rural Development  
Pennsylvania

**PN 329 (2033-A)**  
**February 6, 2012**

**SUBJECT: Protection of Personally Identifiable Information (PII), Sensitive But Unclassified Data (SBU), Government Furnished Equipment (GFE) and Authorization to Remove Files and GFE**

**TO: All Employees**  
**Rural Development, Pennsylvania**

**PURPOSE/INTENDED OUTCOME:**

Rural Development's policy is to protect PII and SBU data from unauthorized disclosure. This memorandum defines PII and SBU data, outlines responsibilities for protecting the security of the PII and SBU data collected, transmitted, stored and disposed and provides authorization for the removal of SBU data to an alternate worksite. The contents of this Procedure Notice combine the guidance of various documents already published.

**IMPLEMENTATION RESPONSIBILITIES:**

**A. Definitions:**

1. PII is any collection, item or grouping of data about an individual/entity maintained by an agency which can be used to uniquely identify that individual. It can include personal information (i.e. full names, maiden names, streets or email addresses, telephone numbers, taxpayer identification numbers (TINs), social security numbers (SSN), employer or employee identification numbers (EIN), place or date of birth, educational information, financial information (transactions, credit card numbers, bank account numbers), employment, medical and/or criminal histories.

For example, a birthplace is not sensitive data on its own; however if combined with a name or other identifiable item it may become sensitive data. Good reasoning must be used in order to prevent PII disclosure when handling such data as it is unfeasible to

**FILING INSTRUCTIONS:**  
**Preceding Instruction 2033-A**

One Credit Union Place • Suite 330 • Harrisburg, PA 17110-2996  
Phone: (717) 237-2299 • Fax: (717) 237-2191 • TTY/TDD & Voice: 711; TTY/TDD only: (717) 237-2261  
Web: <http://www.rurdev.usda.gov/pa>

Committed to the future of rural communities.

"USDA is an equal opportunity provider, employer and lender."  
To file a complaint of discrimination write USDA, Director, Office of Civil Rights, 1400 Independence Avenue, S.W., Washington, DC 20250-9410 or call (800)795-3272 (voice) or (202) 720-6382 (TDD).

define the level of sensitivity for every possible combination of data. Dependent upon the grouping of information, PII data is less or more sensitive.

One grouping of data which must always be protected is a TIN/SSN/EIN when combined with the individual's or entity's name.

2. SBU includes PII data, funding and budget documents, For Official Use Only documents, contract documents, grant and loan files, and Essential Records.

RD defines Essential Records as any original record document which provides evidence of indebtedness or obligation to RD. Essential Rural Development Records require maximum protection at all times (2033-A). These records are to remain in a locked cabinet except when the record is in use. Essential Records include but may not be limited to:

- Promissory Notes of any kind (renewal, consolidation MFH, etc.);
- Assumption Agreements;
- Grant Agreements;
- Repayment Agreements of any kind (accelerated, subsidy, etc.);

## **B. Encrypting Sensitive Data**

SBU data must be encrypted when stored or transmitted electronically (DM 3550-002). Attachment A provides the process for encryption. The process may also be located via [http://rdirm.sc.egov.usda.gov/documents/memos/IH/Storing\\_Sensitive\\_Data\\_sgg3.doc](http://rdirm.sc.egov.usda.gov/documents/memos/IH/Storing_Sensitive_Data_sgg3.doc) beginning on Page 5.

## **C. Sharing Encrypted Data**

1. SharePoint – the ability to upload information is restricted. SharePoint shall not be used for the storing or sharing of SBU data.
2. Email – when sharing any sensitive information through email, employees must adhere to the following guidance to ensure its protection:
  - Encrypt the file according to the instructions in item B;
  - Attach the encrypted file to the email;
  - Transmit the email only to those personnel in need of the data; and
  - Notify the recipient through a separate email or telephone call of the password.
    - Do not supply the password in the same email which contains the encrypted file;
    - The subject of the email containing the password will not draw attention to the email's content. For example, do not subject the email "Password for Encrypted File", etc.
3. Hard-Copy shipping – when sharing hard-copy information through mail services, employees must adhere to the following guidance to ensure its protection:
  - Mark physical documents containing PII as "SBU/PII – Disseminate on a Need-to-Know Basis Only";
  - Double wrap the documents; and

- Send the package via an approved carrier which offers the ability of package tracking (pick-up, transportation, delivery, etc.).
4. Portable Media shipping – when sharing SBU data on portable media devices (PMD) through mail services, employees must adhere to the following guidance to ensure its protection:
- Encrypt the data according to the instructions in item B;
  - Burn the encrypted file to the PMD;
  - Double wrap the PMD;
  - Send the package via an approved carrier which offers the ability of package tracking (pick-up, transportation, delivery, etc.);
  - Transmit the password via separate communication (telephone, email, certified mail). If sending the password via email, please refer to item C2.

#### **D. Working with SBU**

1. PA RD Website – all information is published through the Public Affairs Specialist. All information is examined through an approval process ensuring SBU/PII data is not compromised.
2. Telecommunications – in general, SBU data should not be discussed on phones. SBU data should never be discussed on cell phones; cells normally do not offer secured transmissions which allows for easy interception.
3. Removal from Office – SBU data, which includes dockets and files, should not be removed without signing such items out. Attachment C provides the method for signing out dockets, files or other SBU data.
4. Electronic Data and Hard Copies – SBU data must not be left unattended on computer screens or work stations either in the traditional office or at the alternate work site. SBU data must be secured and stored properly when not in use.

#### **E. Electronically Storing SBU**

1. Government Furnished Equipment (GFE) – if SBU data is stored on a government computer, the data must be encrypted. Any SBU data not possible to encrypt must be stored on a portable media device (i.e. discs, etc.) and kept in a locking office, cabinet or desk drawer.
2. Personally Owned (Non-GFE) Equipment – SBU data related to or obtained from performance of official duties will not be stored on non-GFE or personally owned equipment; this data may only be stored on GFE.

#### **F. Disposing of SBU**

1. Thumb or External Hard Drives – reformatting of these devices will dispose of SBU and all data. Ensure the device is connected to a USB port, and follow the path *Start, My Computer*, right click on the *USB Drive Letter*, *Format*, *Start*.

2. CDs and DVDs – if the device cannot be entirely reformatted to completely clear the data, it should be shredded.
3. Hard Copies – paper copies of SBU data must be shredded; never place these items in the regular trash receptacles.

#### **G. Authorization to Remove Files/Equipment from the Official Duty Station**

1. It is often necessary for an employee to remove an official file containing PII from their duty station in order to perform their job duties (i.e. field visits, inspections, telework).
2. The October 26, 2011, memorandum “Minimum Safeguards for Protecting Personally Identifiable Information (PII) and USDA PII Training” states that the removal of PII, regardless of the form, from the workplace without prior written authorization from the USDA unit manager or other authorized senior agency official is strictly prohibited. This Procedure Notice provides authorization for the removal of files and/or associated documents by PA RD employees; however, classified documents are not included in this approval.
3. Attachment B will be used to track any Government Furnished Equipment (GFE) that is removed from the official duty station. It will be maintained at the employee’s desk in a location that is easily visible. When the sheet has been completely filled, it will be maintained in the Office’s property files.
4. In order to provide a consistent means of tracking the movement of files, Attachment C must be utilized whenever files are removed from an office. The Attachment should be centrally located and/or visible within the office in order to easily identify the whereabouts of PII information that has been removed from the office and will be retained annually in Operation File 2045-A.

#### **H. Incident Reporting**

1. A security incident is defined as any event, whether intentional or accidental, which may compromise security. It includes any loss or unauthorized access to data or computer systems; disclosure of sensitive information; loss of information, data, hardware and/or software; fraud, embezzlement, computer virus; or other suspicious activity.
2. Employees must report security incidents to the RD Information Systems Security Staff Point of Contact (ISSS-POC) in the State Office, the supervisor, and the ITS representative. The ISSS-POC will collect information for the Incident Response Team. Once information is collected related to the incident, the ISSS-POC will provide additional guidance regarding any further actions necessary.

THOMAS P. WILLIAMS  
State Director

Attachments

## Encryption Instructions

### Encrypting Files Using WinZip

To encrypt files using WinZip perform the following steps:

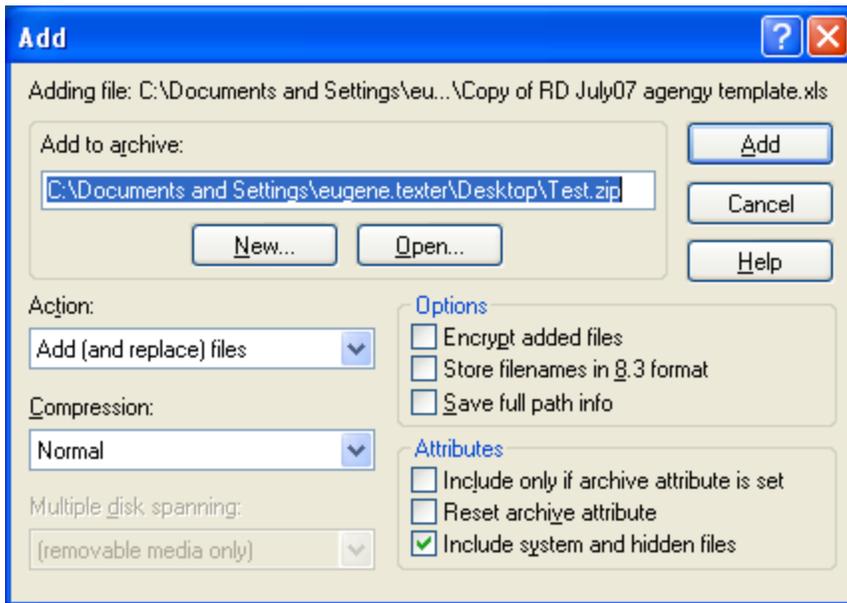
1. Create a new WinZip file, right click on your desktop select New > WinZip file.



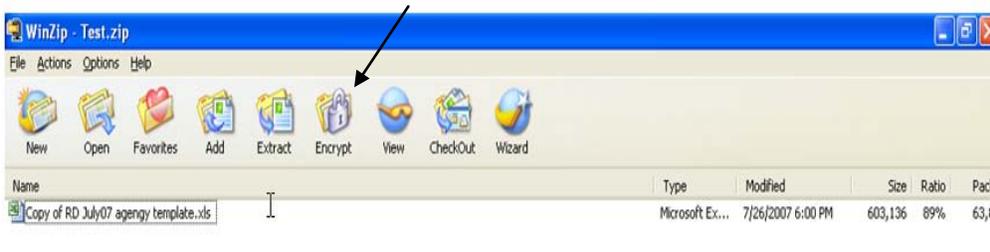
2. Rename the new file. The file extension must be .zip.



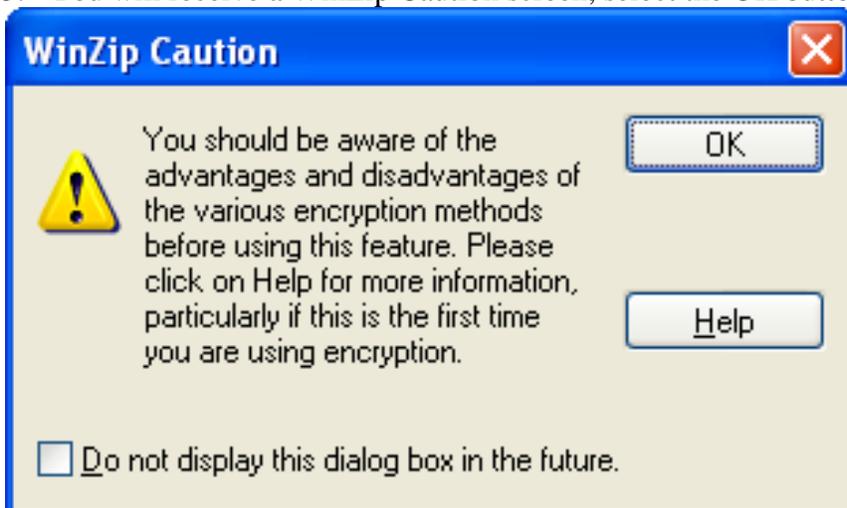
3. Add files to the new WinZip file, drag and drop any file to the folder. You may select multiple files to do it all at once or individual files. Once you drag them to the folder the screen below will appear – select the Add button.



4. The file is now added to the WinZip file. Open the WinZip file and select the Encrypt icon from the WinZip toolbar.



5. You will receive a WinZip Caution screen, select the OK button.



6. You will now receive the Encrypt screen, enter the password you wish to use and then re-enter it to confirm. **Note:** Strong passwords must be used; minimum of 12 characters in password, Alphanumeric and special must include a number, upper and lower case letter.

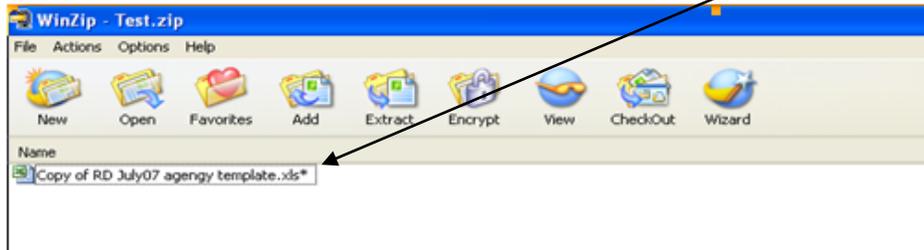


Make sure you use you select at least 128 bit Advanced Encryption Standard (AES) encryption: [128 Bit AES encryption](#). This is the minimum encryption standard accepted by USDA.

7. Select the OK button.



8. Your document is now encrypted and is indicated by the asterisk \* at the end of the document



9. The WinZip file may now be emailed, burned to Compact Disk (CD), flash-drive, etc... Ensure you either call the recipient and tell them the password or email the password in a separate email.

## Microsoft Office 2007 Application Encryption Instructions

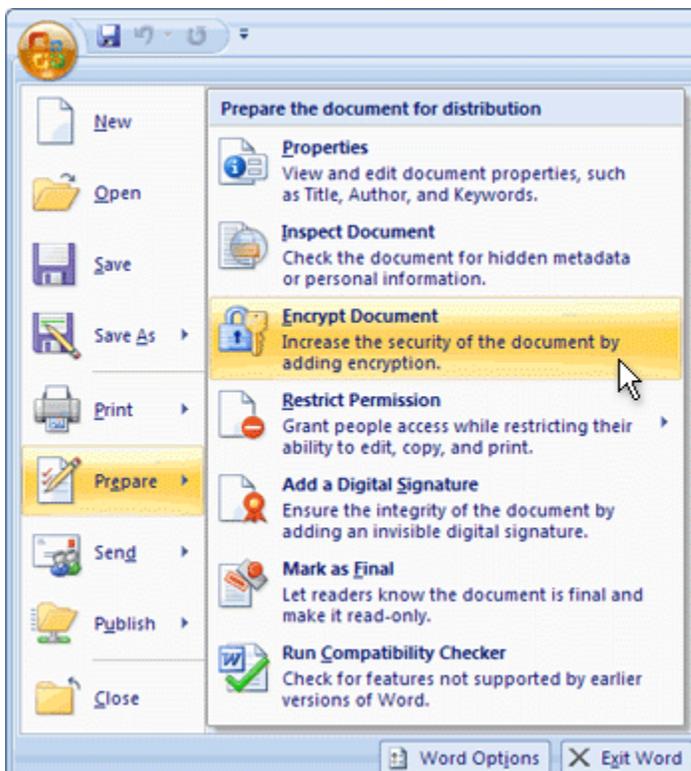
**Note:** These instructions apply to Microsoft Office 2007 only. Previous versions do allow for encryption.

### Microsoft Word

#### Set a password in a Word document

To encrypt your file and set a password to open it:

1. Click the Microsoft Office Button , point to Prepare, and then click Encrypt Document.



2. In the Encrypt Document dialog box, in the Password box, type a password, and then click OK.

You can type up to 255 characters. By default, this feature uses AES 128-bit advanced encryption. Encryption is a standard method used to help make your file more secure.

3. In the Confirm Password dialog box, in the Reenter password box, type the password again, and then click OK.
4. To save the password, save the file.

### Remove password protection from a Word document

Use the password to open the document.

1. Click the Microsoft Office Button , point to Prepare, and then click Encrypt Document.
2. In the Encrypt Document dialog box, in the Password box, delete the encrypted password, and then click OK.
3. Save the file.

### Set a password to modify a Word document

In addition to setting a password to open a Word document, you can set a password to allow others to modify the document.

1. Click the Microsoft Office Button , click Save As, and on the bottom of the Save As dialog, click Tools.
2. On the Tools menu, click General Options. The General Options dialog opens.
3. Under File sharing options for this document, in the Password to modify box, type a password.
4. In the Confirm Password dialog, re-type the password. Click OK.
5. Click Save.

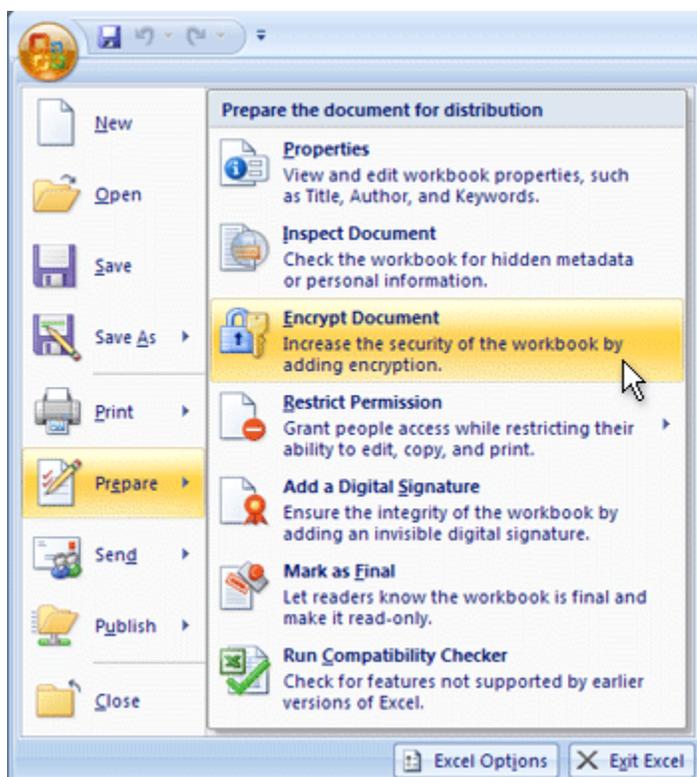
**NOTE:** To remove the password, repeat these instructions and then delete the password from the Password to modify box. Click Save.

## Microsoft Excel

### Set a password in an Excel spreadsheet

To encrypt your workbook and set a password to open it:

1. Click the Microsoft Office Button , point to Prepare, and then click Encrypt Document.



2. In the **Password** box, type a password, and then click OK.

You can type up to 255 characters. By default, this feature uses AES 128-bit advanced encryption. Encryption is a standard method used to help make your file more secure.

3. In the **Reenter password** box, type the password again, and then click **OK**.
4. To save the password, save the file.

### Remove password protection from an Excel spreadsheet

1. Use the password to open the spreadsheet.
2. Click the Microsoft Office Button , point to Prepare, and then click Encrypt Document. In the Encrypt Document dialog box, in the Password box, delete the encrypted password, and then click OK.
3. Save the spreadsheet.

## Set a password to modify an Excel spreadsheet

In addition to setting a password to open an Excel spreadsheet, you can set a password to allow others to modify the spreadsheet.

1. Click the Microsoft Office Button , click Save As, and on the bottom of the Save As dialog, click Tools.
2. On the Tools menu, click General Options. The General Options dialog opens.
3. Under File sharing, in the Password to modify box, type a password.
4. In the Confirm Password dialog, re-type the password. Click OK.
5. Click Save.

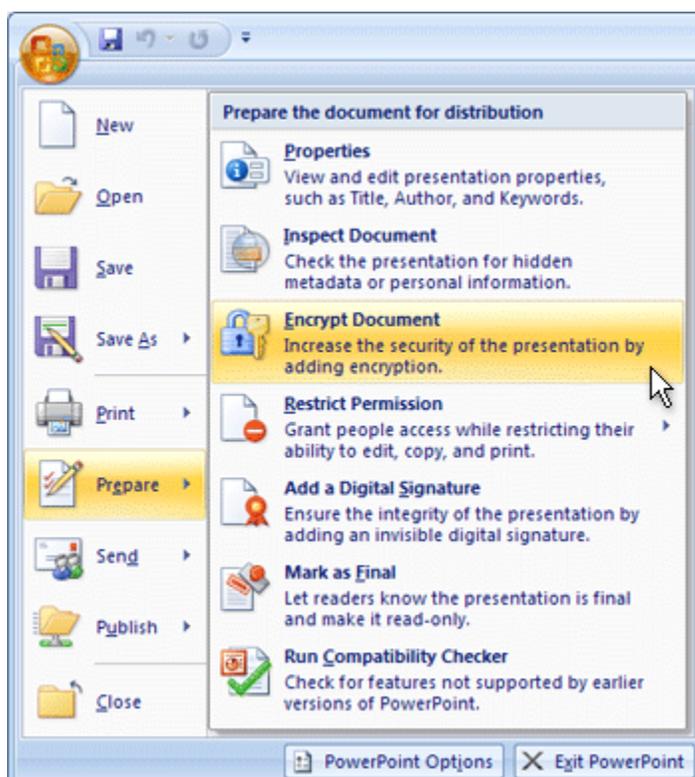
**NOTE** To remove the password, repeat these instructions and then delete the password from the Password to modify box. Click Save.

## Microsoft PowerPoint

### Set a password for a PowerPoint presentation

To encrypt your presentation and set a password to open it:

1. Click the Microsoft Office Button , point to Prepare, and then click Encrypt Document.



2. In the Password box, type a password, and then click OK.

You can type up to 255 characters. By default, this feature uses AES 128-bit advanced encryption. Encryption is a standard method used to help make your file more secure.

3. In the Reenter password box, type the password again, and then click OK.

4. To save the password, save the file.

### Remove password protection from a PowerPoint presentation

1. Use the password to open the presentation.
2. Click the Microsoft Office Button , point to Prepare, and then click Encrypt Document.
3. In the Encrypt Document dialog box, in the Password box, delete the encrypted password, and then click OK.
4. Save the presentation.

### Set a password to modify a PowerPoint presentation

In addition to setting a password to open a PowerPoint presentation, you can set a password to allow others to modify the presentation.

1. Click the Microsoft Office Button , click Save As, and on the bottom of the Save As dialog, click Tools.
2. On the Tools menu, click General Options. The General Options dialog opens.
3. Under File sharing settings for this document, in the Password to modify box, type a password.
4. In the Confirm Password dialog, re-type the password. Click OK.
5. Click Save.

**NOTE** To remove the password, repeat these instructions and then delete the password from the Password to modify box. Click Save.



