COMPASS GROUP, NORTH AMERICA
SYSTEMS SECURITY

Encrypting Data Files for Sending Via E-mail

Version 2.0

Introduction

This document is designed to offer assistance in encrypting and compressing data files that are to be sent to a trusted source via E-mail. It will describe the process for using the WinZip application that is standard on the Compass image to compress and encrypt files such as spreadsheets, documents, and text files so that they are easier to deliver via e-mail. While this method adds a basic level of security over sending an unencrypted data file as an e-mail message attachment, it is not intended as a solution for distributing sensitive or confidential information via the Compass e-mail system. It is still a violation of the Corporate Information Security Policy to distribute such information, as stated in the following excerpt from the "Acceptable Use For Information Technology Systems" policy.

Compass Group Security Policy

As per the "Acceptable Use For Information Technology Systems" policy, page 6-16 of the "Compass Group Information Systems Security Policy":

B. Confidential, Sensitive, and Personal Identity Information

1. Confidential Information: Users shall not disclose, via E-mail, Internet, or any form of electronic communication, any confidential or proprietary information regarding Company activities to any party that does not have authority from Company management to access the information and a need to know. This includes, but is not limited to, copyrighted materials, trade secrets, and financial information. All such information is the sole property of the Company. In addition, users shall refrain from sending confidential, proprietary, or private Company information via electronic mail or over the Internet/Intranet.

Users shall observe confidentiality obligations with respect to Company software, documentation and all forms of internal information. This information cannot be sold and/or transferred to any non-Company party for any purposes without written authorization by Company management.

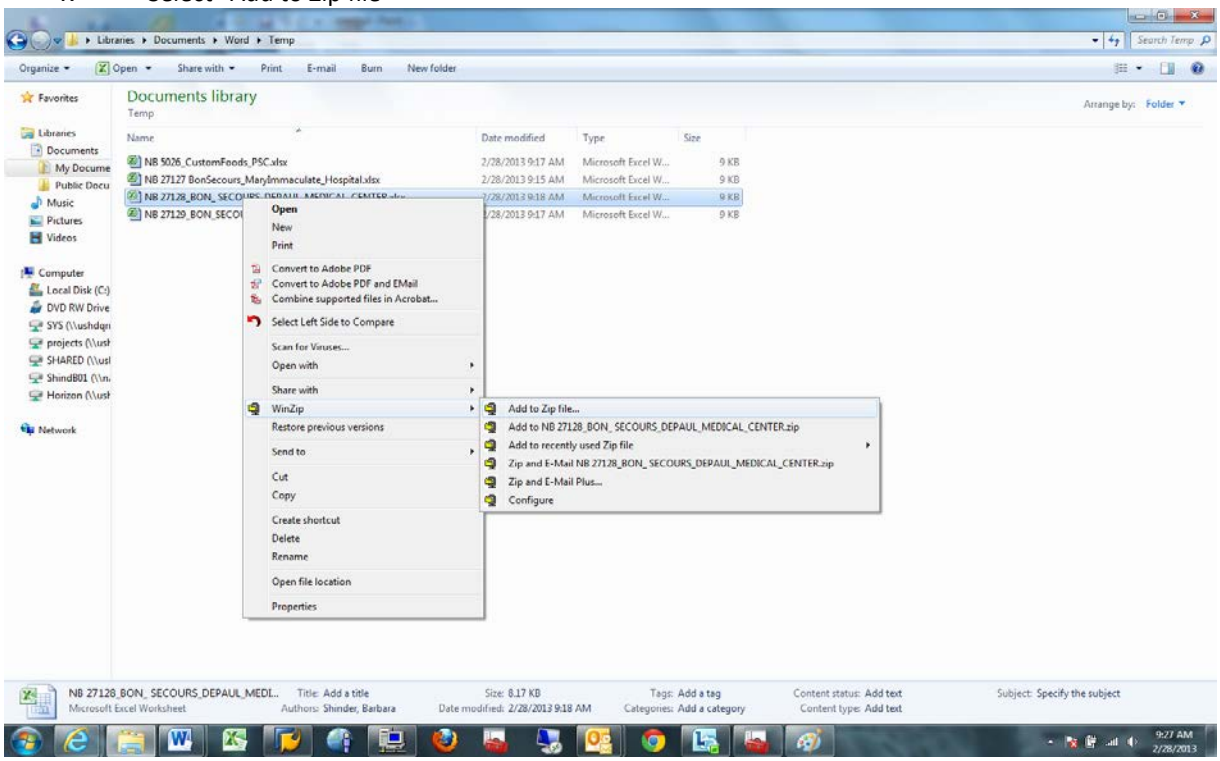
2. Sensitive Information: "Sensitive Information" should not be sent via E-mail, posted on or transmitted over the Internet, or stored on mobile electronic storage media (such as thumb drives) or on data storage files accessible company-wide or by the public. For the purposes of this Policy, "Sensitive Information" shall include, without limitation, classified Company management or financial reports, communication of a litigious nature, employee relations investigative information, or other information that could reveal the Company's private business information or create litigious exposure.

3. Personal Identity Information: For the purposes of this Policy, "Personal Identity Information" shall include, without limitation, social security numbers, drivers license numbers, state identification card numbers, credit or debit card numbers, bank account numbers, passport numbers, alien registration numbers, health insurance identification numbers, user IDs and passwords. Personal identity information shall not be sent via E-mail, or posted on or transmitted over the Internet without approval from ISS. Personal Identity Information should never be stored on mobile electronic storage media (such as thumb drives) or on data storage files accessible company-wide or by the public.

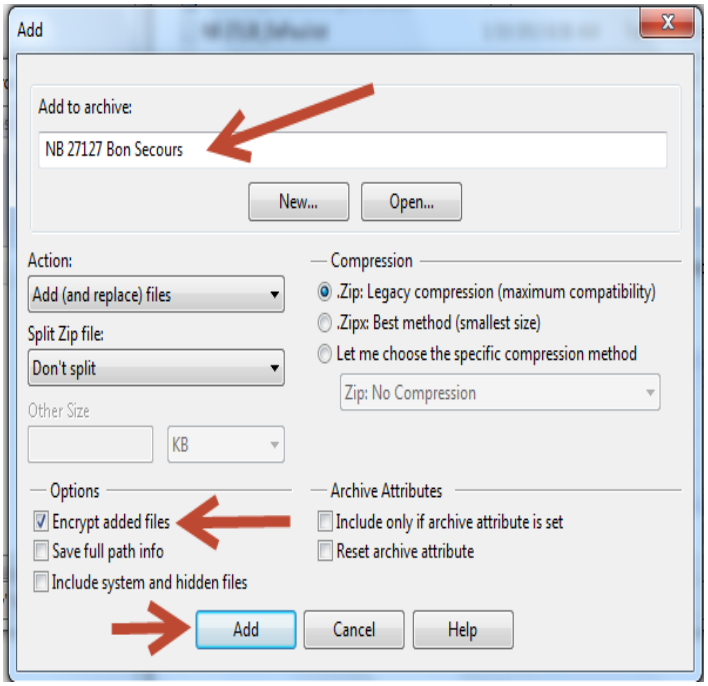
COMPASS GROUP, NORTH AMERICA
SYSTEMS SECURITY

Procedures for Encrypting Data Files

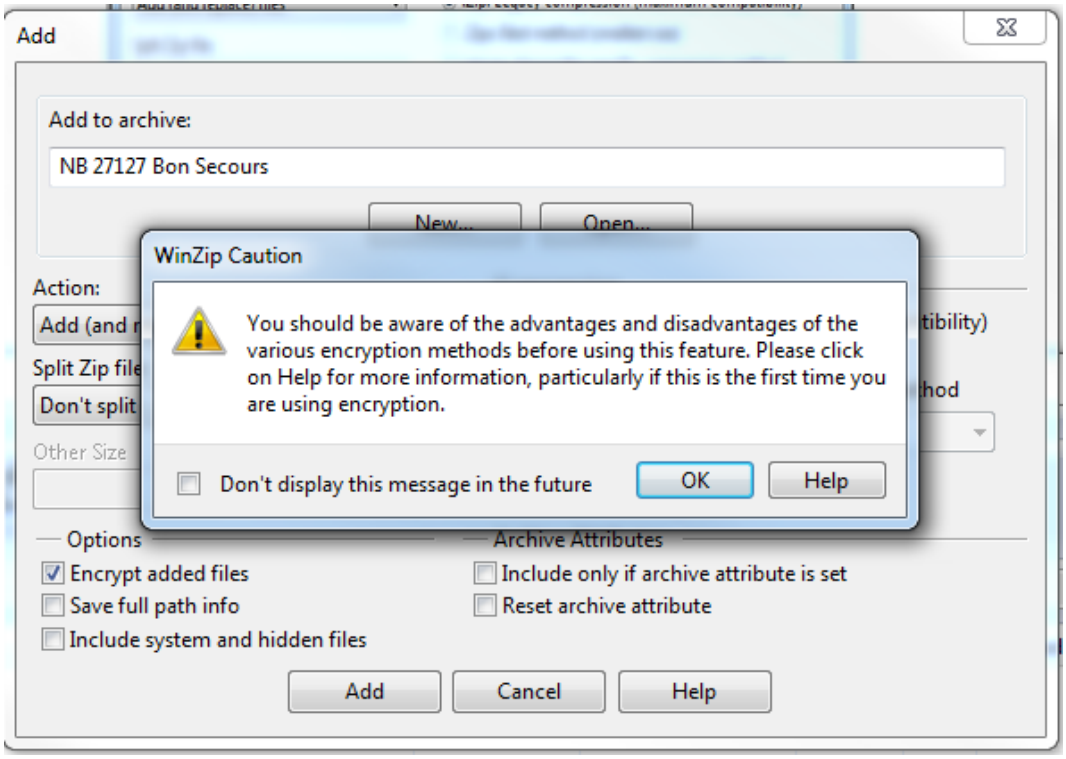
1. Select the file you want to zip
2. Then right click
3. Select WinZip
4. Select “Add to Zip file”



5. Enter what you want the output file to be named in “
6. Add to archive:”Under “Options”, check the box entitled “Encrypt added files”
7. Select “Add” at the bottom



8. If the following message pops up, click OK



9. You will be prompted to enter a password
10. Enter a password that meets the following requirements:
    a. At least 8 characters in length
    b. Be random, no dictionary or common words, no names
    c. A mixture of upper and lower case, as well as numbers and special characters (*, #, %, and so on)
11. Re-enter the same password for verification
12. Make sure that 256-Bit encryption is chosen

13. Click OK
14. Email the .zip file that you just created and then phone the recipient of the email with the password. DO NOT EMAIL THE PASSWORD.