Procedures for Encrypting Data

The *Data Handling Procedures* require that the storage of sensitive data in some locations be encrypted. They also require that when emailing some sensitive data, the attachments be encrypted. This document gives instructions and guidance on WCU supported methods of encryption. Refer to the *Data Handling Procedures* for information about encryption requirements.

- **Encrypting Folders**
    - In general, folder encryption is not supported at WCU. If a folder of files needs to be encrypted, it should be stored as a password-protected Zip file.
    - If there is a business need to store Red & Orange data on a routine basis, you should contact the Help Desk and request a SecureShare folder.
- **Encrypting Files**
    - You should choose to use file encryption if you have an individual file with RED or ORANGE data and the folder is in the Medium Security Zone (Mercury, WCU-managed end-user computers, OneDrive and SharePoint).
    - Individual file encryption supported by WCU is accomplished by password protecting a file which also encrypts the file. The following is a list of applications that support this (may need to purchase licenses):
        - Microsoft Office applications
        - Adobe Acrobat
        - WinZip Pro (can be used for one or more files in a single Zip file)
    - The methods used to password protect files vary by application. You should contact the Help Desk if you need assistance with this.
    - Passwords for encrypted files can be shared with others that need to access the information.
    - Passwords need to be securely saved to ensure the file is recoverable. If a password is forgotten or lost the data in the file will be lost.
- **Encrypting Email**
    - Sensitive data should **not** be included in the body of an Email message.
    - If you need to Email sensitive data, it should be put in an attachment and the attachment should be password-protected using one of the methods mentioned above for encrypting files.
    - Do not send a password-protected file as an attachment via Email and include the password in the same message.
    - Emailing Red data via an encrypted attachment requires prior approval from University Counsel.