FCC Computer Security Notice

JUNE 2002

SECURING PORTABLE ELECTRONIC MEDIA

This month's Computer Security Notice focuses on how you can provide adequate protection of portable electronic media (e-media) that you create from time to time to move data from the office to your home or vice-versa. Compact disks, CD-ROMS, zip drives, floppy diskettes and tapes are all considered portable e-media. There are several precautions you can take to protect FCC data.

The protection of computer generated information is critical as part of today's Homeland and computer security focus. Losing control of such data can mean millions in compromised information, potentially swaying the economic impact of the Commission's agenda items or adversely affecting the reputation of the FCC by not adequately protecting information for which you are entrusted.

Knowing how to properly protect e-media will provide you with the edge needed to keep your information secure.

Password protect or encrypt the data. This will keep it from easily being viewed by someone who might gain physical access to the e-media. It is also the most practical way to protect your information. To support the process of password protecting files you store to e-media, FCC users can access and use the WinZip utility provided on your desktop. Additional information on how to use the WinZip feature is provided on page two of this document.

Physical protection of portable e-media is *key*. If no one else can gain access to the physical device, they cannot access the information. Always be aware of where the e-media is located and make sure it is secure. Also, properly labeling the e-media serves to remind you of its importance.

Mother Nature can also have an adverse affect on your e-media. Summer's sweltering heat can affect the information's readability. Beware of extreme temperatures! Also keep the e-media out of reach of small hands (or paws) and away from beverage or food items, which can also affect the availability of the information.

Simply throwing your CD-ROM or diskette out with the trash is not a secure method of destruction. Portable e-media is most often destroyed by crushing, breaking, incinerating, melting or shredding. For those in the Portals complex, Washington, DC, the Security Operations Group, Room 1-B458, collects e-media for destruction through our contract service provider. Remote facilities should consider a similar process for e-media destruction.

FCC staff should not forward e-media via the US Postal Service because the media will likely become corrupt as part of the irradiation process.

In summary, be aware of the information you store on portable e-media. Make sure to it when containing sensitive or critical FCC data. Report the loss of such information to your supervisor and the Computer Security Officer *immediately*.

COMPUTER SECURITY TIP OF THE MONTH

MAKE SURE THAT YOUR DATA IS BEING BACKED UP. CENTRALLY MANAGED COMMISSION FILE SERVERS & ITS DATA ARE BACKED UP NIGHTLY BY OUR IT OPERATIONS GROUP. IT IS YOUR RESPONISIBILITY TO BACKUP DATA STORED ON YOUR LOCAL PC DRIVES.

FOR ADDITIONAL INFORMATION ON FCC COMPUTER SECURITY

- The FCC Computer Security Program at: http://intranet.fcc.gov/omd/itc/csg/index.html
- The Management of Non-Public Information at: http://intranet.fcc.gov/omd/perm/directives/1139.html

NOTE FROM THE FCC COMPUTER SECURITY OFFICER

The FCC has placed a significantly high emphasis on the protection of its computer-based data. Countless hours are devoted to ensure that in-place controls remain effective. By downloading information off of the FCC network and storing it to portable e-media, the FCC system user no longer has network controls available to protect the data. It is now the responsibility of the FCC user to ensure secure use of the media and provide its protection until it has been destroyed.

USING WINZIP TO PROTECT YOUR E-MEDIA DATA

WinZip allows you to compress large data files. Also, you can secure these files with a password.

WinZip uses the industry standard Zip 2.0 encryption format. Password protecting files in a Zip file provides a measure of protection against casual users viewing the files.

> ***Note**: If you require **strong** encryption, we recommend you use specialized encryption software instead of the Zip 2.0 encryption format.*

Follow these steps to password protect files to be copied to a portable e-media device:

Click **Start: Programs: WinZip.**
Click the **New** button.
Change the Directory to the location where you want the Zip file(s) to be saved.
Type the filename for the Zip file and then click **OK**.
Select all files to be added to the Zip File.
To password protect the selected files, click on the **Password** button.
Type a password then click **OK.** Re-type the password and then click **OK.**
To add all selected files to the Zip file click the **Add** button.

***Note:** All files with a password will have a plus(+) sign to the right of these files.*
Choose **File: Exit** to Close the WinZip program.

To extract or access your password protected Zip files.

Double click on the Zip file that you want to open.
Select the file(s) that you want to extract from the zip file.
Click the **Extract** button.
Select the destination of your files and then click **Extract**. You will be prompted to enter the password.
Type your password then click **OK**.
The files are extracted to the destination directory.
Choose **File: Exit** to close the WinZip Program.