FCC Computer Security Notice

March 2003

Password Protecting Non-Public/For Internal Use Only FCC Information

The FCC maintains an aggressive use of technology to increase productivity. The use of portable electronic devices capable of processing and storing information remain key to this success. To support our technology use, the FCC has placed a significant emphasis on the protection of its Non-Public/For Internal Use Only information (see FCC Instruction 1139, Management of Non-Public Information for definition). In June 2002 this office released a Computer Security Notice discussing Securing Portable Electronic Media. This month's notice is intended to supplement and support the June '02 notice.

From time-to-time, Non-Public/For Internal Use Only information must be downloaded and stored to portable electronic devices [i.e., laptop computer, telecommuting or personally-owned personal computer (PC) , personal digital assistant (PDA), RIM pager or similar device.]

While it is not absolutely necessary to password protect all portable devices, it is policy that portable devices containing FCC Non-Public/For Internal Use Only information be password protected.

Once downloaded, security of the information stored on the portable device becomes the *sole* responsibility of the person in possession of the device. As discussed in the June '02 notice, physical protection of portable electronic media [information] is *key*. If no one other than the owner can gain access to the physical device, they cannot access the information.

A summary of the FCC password policy [in red block] is offered as a guide to help you select strong passwords to protect FCC information. If you currently store FCC Non-Public/For Internal Use Only information on a portable device, you must apply a password to either the device or the file to ensure its security.

FCC Password Policy (*Summary*)

1. Password protect all portable devices or specific files containing Non-Public/For Internal Use Only information when being stored to portable device.
2. Select a strong password, i.e., not your name or initials, or words easily found in a dictionary. Use a password with a minimum length of six characters consisting both alpha/numeric and special characters. Examples include "B4time%" or "2Brnot2B!".
3. Do not share or write down your password and do not select to auto save your password as part of the portable device log-on sequence.

Special Note: Effective immediately, you are required to seek permission of the Bureau or Office (B/O) database owner prior to downloading database information to a portable device, if you intend to do so. As an example, you are not required to gain permission to download your email to a RIM pager or your home PC. However, you are required to request permission to download an FCC managed database to your laptop, home computer or other portable device. The B/O database owner will make the determination if the information you intend to download is sensitive to the mission of the FCC.

The ITC is developing a form that will allow you to certify that you have requested permission to download Non-Public/For Internal Use Only information from the database owner and that the information stored on portable devices is secured using strong passwords. The form will be distributed via a follow-up Computer Security Notice once completed. We expect that most Commission staff may be required to sign the form.

To ensure that you are able to manage passwords for the portable device[s] assigned to you, Tip Sheets on securing a variety of portable electronic devices have been prepared for your use and are referenced on page 2 of this notice.

As always, you are encouraged to reference the Commission's directives on computer and information security. Links are provided below.

Computer Security Tip of the Month

IMMEDIATELY report suspected theft/loss of FCC issued equipment to the Security Operations Center, (202) 418-7884.

YOU CAN ACCESS FCC INSTRUCTION 1479.2, FCC COMPUTER SECURITY PROGRAM DIRECTIVE AND ADDITIONAL INFORMATION ON PASSWORD CONTROLS AT:

- http://intranet.fcc.gov/docs/omd/itc/csg/1479-2.pdf

YOU CAN ACCESS FCC INSTRUCTION 1139, MANAGEMENET OF NON-PUBLIC INFORMATION AT:

- http://intranet.fcc.gov/omd/perm/directives/1139.html

YOU CAN ACCESS ADDITIONAL INFORMATION ABOUT THE FCC COMPUTER SECURITY PROGRAM AT:

- http://intranet.fcc.gov/omd/itc/csg/index.html

YOU CAN ACCESS THE JUNE 2002 COMPUTER SECURITY NOTICE ON SECURING PORTABLE ELECTRONIC MEDIA AT:

- http://intranet.fcc.gov/docs/omd/itc/csg/notices/remove-media.pdf

Password Protecting Sensitive Information
(Links - Setting Passwords on Portable Devices)

The following links provide step-by-step instruction for setting passwords on a variety of portable devices and Microsoft desktop applications:

- Tip Sheet—Password Protecting ComPaq iPAQ: http://intranet.fcc.gov/docs/omd/itc/csg/tips/iPAQ.pdf 
- Tip Sheet—Password Protecting m505 Palm Pilot: http://intranet.fcc.gov/docs/omd/itc/csg/tips/Palmm505.pdf 
- Tip Sheet—Password Protecting Handspring Visor Prism: http://intranet.fcc.gov/docs/omd/itc/csg/tips/HandspringVisor.pdf 
- Tip Sheet—Password Protecting HP Jornada: http://intranet.fcc.gov/docs/omd/itc/csg/tips/HPJornada.pdf 
- Tip Sheet—Password Protecting RIM Pager: http://intranet.fcc.gov/docs/omd/itc/csg/tips/rim.pdf 
- Tip Sheet—Password Protecting Microsoft Word Document: http://intranet.fcc.gov/docs/omd/itc/csg/tips/word.pdf 
- Tip Sheet—Password Protecting Microsoft Excel Workbook/document: http://intranet.fcc.gov/docs/omd/itc/csg/tips/excel.pdf 
- Tip Sheet—Password Protecting Microsoft Access Document: http://intranet.fcc.gov/docs/omd/itc/csg/tips/access.pdf 
- Tip Sheet—Password Protecting Microsoft PowerPoint Presentation/document: http://intranet.fcc.gov/docs/omd/itc/csg/tips/ppt.pdf 
- Tip Sheet—Password Protecting Microsoft Project: http://intranet.fcc.gov/docs/omd/itc/csg/tips/project.pdf