FCC Computer Security Notice

AUGUST 2002

MINDING YOUR FCC NETIQUETTE

FCC policy states that you are to use systems for authorized use only and should have no expectation of privacy. This type of policy is typical within the Federal government.

The FCC provides Internet capability because it is considered an extremely valuable resource to facilitate your work. You are encouraged to explore the Internet which gives an awareness of the depth and breath of the information superhighway.

While Internet use is encouraged, it is the Commission's responsibility to monitor and manage its use. There are clearly do's and don'ts when using the FCC Internet as outlined in FCC Computer Security Program Directive 1479.2. All FCC users should be aware of proper network etiquette, also known as "*Netiquette*".

It *is* acceptable to use the FCC Internet for limited personal use during non-work time with the understanding that you will use good judgment in selecting the computer sites you choose to visit.

1479.2 states that your Internet usage should have "minimal impact on the Federal Government." Meaning that your use should not "conflict with the performance of your official duties or the mission of the FCC."

You should also consider the "Standards of Ethical Conduct contained in 5 CFR Part 2635 and Part 19 of the Commission's rules" prior to accessing Internet sites.

Sites that might cause embarrassment to the FCC or have an adverse public reaction should be avoided. Internet sites containing sexually explicit material must not be accessed using FCC computers. It is your responsibility to be aware of what type of information is contained in the sites that you frequent.

You have heard it before . . . mass mailing, chain letters and sharing .avi (audio/movie) files are prohibited. Never cause congestion, delay or disruption of service to FCC systems. This might be caused by downloading or e-mailing large files to FCC systems. This can degrade the overall performance of the FCC network and potentially cause its shut down.

You are prohibited from launching illegal computer based attacks against other system or to gain unauthorized access to other systems.

FCC computer systems are not to be used for activities that are illegal, inappropriate, offensive to fellow employees or to the public. Such activities include messages of hate based on a persons race, creed, religion, color, sex, disability, national origin, or sexual orientation.

Accessing gambling, weapons, terrorist or any other illegal sites is also prohibited.

FCC information should not be posted on publicly accessible sites without permission from appropriate FCC staff.

FCC systems log your activity when using FCC provided Internet service. Using the logs, one can determine how long you visited a site and whether or not you returned. The information is archived for several months and can be recalled as needed.

The repercussions for violating FCC policy on Internet use can be severe. Typically, violations of FCC policy are managed within the Commission. Violations of Federal and state law are coordinated between the Office of the Inspector General and affected law enforcement jurisdictions.

Every user on the FCC network is expected to use the Internet wisely and with professionalism. Exercise your *best* judgment.

COMPUTER SECURITY TIP OF THE MONTH:

AN UNATTEND PC IS VULNERABLE TO POTENTIAL UNAUTHORIZED USE. MAKE SURE TO ENGAGE YOUR PC'S SCREEN SAVER WITH PASSWORD TO PROTECT YOUR FCC LOGIN ACCOUNT AND ASSOCIATED PERMISSIONS.

YOU CAN REFERENCE ADDITIONAL INFORMATION ON THE FCC COMPUTER SECURITY PROGRAM AT:

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

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