M E M O R A N D U M

TO: All Locations

FROM: Information Technology Services (ITS)

SUBJECT: **** CRITICAL** VIRUS/WORM THREAT**

Microsoft has announced a virus/worm threat known as “Zotob” that makes use of a Plug-and-Play (PnP) vulnerability to propagate. The worm uses exploit code that targets the PnP issue, it then uses File Transfer Protocol (FTP) to transfer data from the infecting machine. The newly infected machine then becomes an FTP server itself and begins scanning for other vulnerable hosts to infect.

To prevent your site from becoming infected, it is critical that the steps below are followed:

1. Keep ALL site computers turned on 24/7.
2. Set all computers to "automatically update" Microsoft Operating System patches.
3. Insure that **ALL** computers have McAfee EPO client software installed and functioning.
4. Insure that Big Fix is installed on all computers.

All locations are reminded that it is the responsibility of each user to update their VirusScan software. Each user should set their VirusScan software to update DAT files on a weekly basis. Instructions for scheduling the Virus Scan software to update automatically are available from the following website:

http://its.dadeschools.net/virus.htm

If you do not have McAfee installed on your computer, information for obtaining the District's free McAfee Antivirus software is available at the following website:

http://datasecurity.dadeschools.net/

If you have any questions regarding this memo, please call Support Services at 305-995-3705.