M E M O R A N D U M

TO: All MDCPS Network Users

FROM: Information Technology Services (ITS)

SUBJECT: ***** URGENT *** W32/MYDOOM@MM VIRUS**

As you are aware, a new and dangerous email virus or worm called W32/Mydoom@MM has been identified and is propagating itself through the World Wide Web. This virus is a high-outbreak risk mass-mailing worm flooding email servers worldwide. When run, the virus steals email addresses from the infected machine and also automatically generates random email addresses for propagation. This email generation process is similar to technologies spammers use to generate addresses for spam email campaigns. W32/Mydoom@MM generates emails with a spoofed From: address, so incoming messages may appear to be from people you know. Furthermore, the subject line and message body are both randomly generated by the virus.

This worm has been designed to deliver a "denial of service" (DOS) payload starting February 1, 2003, and lasting an estimated two weeks. This is ***very serious*** in that it can and will lock up a school site router to the point that the site will ***not*** be able to access ***any*** services including mainframe applications (payroll, purchasing, ISIS, etc.) as well as the Internet.

ITS has been blocking this virus from the outside Internet since McAfee's first alert on this worm. However, the possibility of the virus entering the MDCPS network through a "back door" (infected laptop etc.) is a very real possibility. To further protect the MDCPS network user community, ITS is aggressively monitoring for the outbreak of this virus within our own MDCPS network. When a school or administrative site becomes infected with this worm, ITS staff will initiate the following process:

1. ITS will prevent the local site's email server from sending/receiving email outside of the local site's network. This will contain the infection to the local site. This includes sites that have Mac email servers.

2. ITS will notify the principal (or site administrator) and computer technician of the situation. Information on how to eradicate the virus will be provided. The burden of doing so will be on the local computer technician.

3. The school must make the effort to "clean" the site environment. When clean, the site must notify ITS via Support Services at 305-995-3705(0). The site will then be "scanned" to determine if the site is healthy enough to open up regular email traffic to the local email server. Steps 2 and 3 will be repeated until the local site is healthy.

4. Beginning Monday, February 2, ITS will notify the appropriate ACCESS Center Superintendent for school sites that becomes infected.

As always, you cooperation is greatly appreciated. If you have any questions regarding this memo, please call Support Services at 305-995-3705(0).