Technology Usage Policy

MAPP either directly or through arrangements with its subsidiaries, currently provides its employees with various electronic tools, such as access to the programs and databases contained on MAPP's internal network, emailcapability on that same internal network, external internet-based e-mail capability, access to external information and systems via the internet, the use of personal computers, network stations and internet devices (referred to collectively as PC in this policy) and the software that resides on them, as well as the use of voice mail. These tools are provided for the sole purpose of assisting employees in the performance of their job duties. Set forth below are MAPP's policies and conditions regarding the use of, and access to, any of the above mentioned tools. These policies apply to all those employees using MAPP's systems, including those who are employed in a contract or temporary basis and may not meet the full legal definition of employee.

GENERAL

1. All hardware and software provided by MAPP or its subsidiaries for use by its employees, as well as all products generated by the employee's use of this hardware and software, is owned exclusively by MAPP.

2. By performing their work related duties utilizing hardware and software owned by MAPP or its subsidiares, employees waive all rights to personal privacy on this equipment.

3. MAPP pays a monthly rate for limited usage of internet services, therefore, employees need to spend their time online wisely. MAPP and its subsidiaries have the right, but not the duty, to monitor any and all aspects of its systems, including but not limited to internet access usage, Sites visited on the internet (even those visited outside of business hours), material downloaded or uploaded by employees, internal and external e-mail sent and received, database and software usage on internal network, PC contents and usage, as well as voice mail systems, to ensure they are being used properly and for business purposes.

4. Using any of these systems in a manner that would violate applicable law and/or any policy is grounds for disciplinary action, up to and including dismissal and/or legal action.

5. MAPP and its subsidiaries will not be responsible for any damages, direct or indirect, arising out of the improper use of any of the systems mentioned above.

6. When printing e-mails or web pages, be sure to print only the page in which you are interested. E-mails and web pages often include pages of computer language that will print out and waste paper and toner.

7. MAPP may amend or revise these policies and conditions from time-to-time. Employees will be provided with written copies of all amendments and revisions to these policies and conditions.

E-MAIL (Internal and External)

1. E-mail sent and/or received on any system or device belonging to MAPP or its subsidiaries is the property of MAPP and is intended solely for carrying out MAPP business. Employees should exercise the same care in drafting e-mail and posting items to newsgroups as they would for any other written communication. Anything created on the computer or the internet may, and likely will, be reviewed by others.

2. MAPP is to be considered as the recipient of all email messages received by employees, regardless of whether the email message was originated from outside or inside of MAPP. Employees should not consider email communications private, despite any such designation by either the sender or recipient.

3. MAPP management can rightfully enter any of the various e-mail systems and review, monitor, copy or delete any or all messages drafted or received by employees, whether they have been held, sent, or received, and disclose such messages to others. The use of passwords to gain access to e-mail is for the protection of MAPP, not the employee; therefore, the employee should not assume that messages are confidential even though a private password is used.

PC AND INTERNET USAGE

1. As a condition of providing employees with access to MAPP PC systems and the internet, MAPP places certain restrictions on workplace use of the internet and those systems. MAPP encourages employee use of the internet and other systems:

• To communicate with fellow employees and clients regarding matters with an employee's assigned duties;

• To acquire information related to, or designed to facilitate, the performance of regular assigned duties; and

• To facilitate performance of any task or project in a manner approved by the employees supervisor.

2. At no time may employees of MAPP visit sites on the internet which are not business related or which are otherwise unacceptable by management including but not limited to the following:

• Sexually oriented sites

• Racist sites

• Sites using explicit language or containing violent images

• Chat rooms

3. Activities in which employees are prohibited from engaging include, but are not limited to:

• Sending, receiving, displaying, storing, viewing, printing or otherwise disseminating material that is, or contains content that is, fraudulent, harassing, illegal, embarrassing, sexually explicit, obscene, excessively violent, intimidating, defamatory or disparaging of others based on their race, national origin, sex, sexual orientation, age, disability, religious, or political beliefs.

Employees encountering such material should report it to their supervisor immediately.

• Displaying, disseminating, downloading, printing, or in any way using copyrighted materials (including articles and unlicensed software) in violation of copyright laws.

• Using any of these systems and resources for the sending, receiving, displaying, storing, viewing, printing or other dissemination of commercial or personal advertisements, solicitations, promotions, destructive programs (i.e., viruses and/or self-replicating code), political material, chain letters and mass mailings that are unsolicited and unrelated to MAPP business, game playing, or any other unauthorized or personal use.

• Loading unauthorized or personal software on MAPP PC devices.

4. All PC devices that access the internet must have up-to-date virus protection software installed and operating at all times. All PC devices that have dedicated access to the internet must also have a firewall program installed and operating at all times. These programs will be specified and provided by MAPP.

5. All material downloaded from any external source MUST be scanned for viruses and other destructive programs before being placed on any of computer systems, networks or other equipment belonging to MAPP or its subsidiaries

6. Employees must comply with all software licenses, copyrights, and all other state and federal laws governing intellectual property and online activity.

7. Because of export restrictions, programs and files containing encryption technology are not to be placed on the internet or transmitted in any way outside of the United States without prior written authorization from the Information Systems Manager.

USAGE OF PROGRAMS AND DATABASES ON INTERNAL NETWORK

The software and databases contained on MAPP network contains confidential and proprietary information. In order to maintain or competitive edge in the marketplace, it is mandatory that all confidential and proprietary information be guarded with the utmost diligence. Either intentional or negligent sharing of this information could jeopardize MAPP financial future, as well as the job security of all MAPP personnel, and it strictly prohibited.

COMPUTER SAFETY PROCEDURES

What is a computer virus?

A computer program file capable of attaching itself to disks or other files and replicating itself repeatedly; typically without user knowledge or permission. Some viruses attach to files so when the infected file executes, the virus also executes. Other viruses sit in a computer's memory and infect files as the computer opens, modifies or crease the files.

What is the difference between a computer virus and a computer work?

Viruses are computer programs that are designed to spread themselves from one file to another on a single computer. A virus might rapidly infect every application file on an individual computer, or slowly infect the documents on that computer, but it does not intentionally try to spread itself from that computer to other computers. In most cases, that's where humans come in. We send e-mail document attachments, trade programs on diskettes, or copy files to file servers. When the next unsuspecting user receives the infected file or disk, they spread the virus to their computer, and so on. Worms on the other hand, are insidious because they rely less (or not at all) upon human behavior in order to spread themselves from one computer to others. The computer worm is a program that is designed to copy itself from one computer to another over a network (e.g. by using e-mail). The worm spreads itself to many computers over a network, and doesn't wait for a human being to help. This means that computer worms spread much more rapidly than computer viruses.

How to identify an email Virus:

The most common way to identify a virus is to pay close attention to the attachment name. Virus attachments often end with .vbs, .ex, or Homepae.html.vbs. Not all viruses have the vbs attachment, so it is important to use your best judgment when opening an attachment. Virus emails can be very difficult to identify as they often come from someone you know and trust. Keep in mind these people may be unaware that they have even spread a virus. The following tools will help you determine the safety of your email.

DO'S:

Delete chain emails and junk email. Do NOT forward or reply to them. These type of emails are considered spam, which is unsolicited, intrusive mal that clogs up the network.

Exercise caution when downloading files from the internet or opening email attachments. Ensure that the source is a legitimate and reputable one.

Make sure that all files are saved within the company folders on network drives, otherwise they will not be backed up. If a virus destroys your files, at least you can replace them with a back-up copy. Backup copies are made at the server and are stored in a separate location form your local PC.

Follow the procedures below to ensure the safety of your computer:

1. Log off of and turn off your computer at the end of each day to ensure that it will receive a fresh virus signature file the next time it is started.
2. Notify management if you see any error or warning messages referring to or generated by McAfee. Normal information messages such as notification that an update has been done do not need to be reopened.
3. Sign off of your machine any time that you will be away from your workstation for long periods of time.
4. Save all of your date in the company file on the server. MAPP does not currently have a procedure for backing up individual clients machines. Therefore, to ensure proper backup, all files should be saved in the appropriate company folder on the server.

DON'TS:

Do Not Open any files attached to an email form an unknown, suspicious, or untrustworthy source.

Do Not Open any files attached to an email unless you know what it is, even if it appears to come from a dear friend or someone you know. Some viruses can replicate themselves and spread through email. Better to be safe than sorry and confirm that they really sent it.

Do Not Open any files attached to an email if the subject line is questionable or unexpected.

Do Not Download any files that are not specifically needed to do their jobs.

Do Not Insert Floppies or CD's from outside MAPP into client PCs without first doing a local virus scan on the appropriate drive. See management for instructions on how to scan disks.