

## Downloads and executables policy

### Overview

#### Purpose

This policy has been established to set guidelines in an effort to clarify the type and nature of files that employees are allowed to download from third-party sources onto their local computers (desktops, laptops, Pocket PCs, Tablet PCs). Although it would be impossible to name every executable or download file in this policy, users should adhere to these guidelines:

1. The download enhances the employee's productivity.
2. The download is from a reputable source.
3. The file does not subject the company to potential liability.
4. **The application, tool, or template has been approved by IT.**

#### Authority

This policy has full support from the MDS's executive steering committee and human resources department. The IT Director administers the policy, which is currently effective for all MDS employees and computer systems.

### Approved downloads

The following is a list of files that employees can download onto their local machines.

#### AOL Instant Messenger

Although the company has not indicated a preferred IM application, instant messaging can offer users a way to quickly and efficiently communicate with coworkers, contractors, and associates. As with all IM applications, users are encouraged to keep personal messaging within reasonable levels.

#### Yahoo! Messenger

Like AOL Instant Messenger, employees can use this application to exchange work-related instant messages. Users are advised not to engage in the chat function of this application as it supports no function of the company. Also allowed are **Trillian**, **MSN Messenger**, and **Yahoo! Messenger**.

#### WinZip

Employees who e-mail large files to contractors and consultants are encouraged to use WinZip, a compression utility.

#### Ad-aware

As employees may unwittingly download adware onto their local machines, applications such as Ad-aware, which scans a user's system for adware, are allowed. Please note: Some useful proprietary applications on the company network are seen as adware by this and other similar applications. Contact the IT department if you have questions about this kind of application.

#### Spybot

Please check with the IT department to see if this will affect any in-house applications.

## **RealOne Player**

Employees can use this application to listen to music and view streaming media at their workstation. Users will take care not to adversely affect other workers and will, for example, keep the volume of the music and other media played on this application within reasonable levels, if they are located in an office.

## **Adobe Acrobat Reader, Adobe Reader**

Users must have this downloaded to view PDF files.

## **Microsoft Windows Media Player, Winamp**

As with RealOne Player, please be courteous toward other employees when playing audio and video files on this application.

## **QuickTime**

Use of this application is allowed.

## **Ebook applications**

This includes Microsoft Reader, Palm Reader, and other third-party applications that allow users to download work-related texts onto their local machines.

## **Antispam applications**

Because spam has become a significant issue for employees, the use of antispam tools and applications is allowed. However, because many of the freeware applications available for download are relatively new, please allow IT to review the application before installing it on your local machine. Some of the applications that are allowed are: Ella for Spam 1.1, Spam Inspector for Outlook 2000/2002 3.1, Spam Butcher 1.5, SpamCatcher 2.6, SpamWeed 1.3.7, Spam Fighter 1.06, SpamCatcher POP, Anti-Spam 2.0, MailWasher Pro 3.1, Ultra Spam Filter 1.5, McAfee SpamKiller 4.0, and Spam Inspector for AOL 3.0.

## Prohibited downloads

The following downloads are not allowed on company computer resources.

### **Kazaa Media Desktop**

Peer-to-peer file-sharing applications have come under scrutiny in recent years for their ability to allow users to share copyrighted material and for the network resources that they consume.

### **iMesh**

As with Kazaa Media Desktop, this application is not allowed because it could facilitate users sharing copyrighted files on the company network. Such applications can also contain third-party applications, so called adware or spyware, that collect information about a user's Web surfing habits, change system settings, or place unwanted advertising on the local computer.

### **Morpheus (all versions)**

Use of this P2P file-sharing program is prohibited.

### **WinMX**

Use of this P2P file-sharing program is prohibited.

### **LimeWire**

Use of this P2P file-sharing program is prohibited.

### **Grokster**

Use of this P2P file-sharing program is prohibited.

### **BearShare**

Use of this P2P file-sharing program is prohibited.

### **ZoneAlarm**

While security is an issue that every employee can help manage, IT does not allow the use of personal firewalls on company equipment.

### **Any third-party screen saver or wallpaper**

This is to prevent images that might be deemed offensive by some staff members from being displayed on company monitors. Employees will use the default screen savers available on their local machines.

### **Games**

Because games provide no benefit to our organization and have a tendency to affect productivity, they are not allowed on company machines. Telecommuters who use their own local machines on which to work are exempt from this policy. However, those who use company-purchased machines must abide by this rule.