

Overview

As an addendum to the company's Acceptable Use Policy—which details the utilization of the company network, the Internet, e-mail, and employees' personal computers—this policy prohibits the use of Peer-to-Peer (P2P) file-sharing applications and goes into effect immediately.

The company's goal with this additional policy is to:

- Realize the maximum productivity from each employee.
- Address any potential liability from instances when employees download copyrighted material.
- Minimize network disruption.
- Protect the network from exposure to malicious code (worm, virus, Trojan horse).
- Protect the company's intellectual property.

Here is an explanation of each issue as it relates to file-sharing applications and our company:

Worker productivity

The ongoing health of the company is contingent upon each worker giving each task his or her maximum attention and effort. Using a file-sharing application to search for files, downloading them onto the company network or a client machine, and reading or playing them at a workstation is not germane to an employee's job duties and does not enhance a worker's productivity. Another issue is the possibility that P2P applications could disrupt software on an employee's workstation.

Liability

Although many materials have been placed on P2P networks with a creator's consent, much of the material (images, software, movies, music, video) has been duplicated from copyrighted materials. Downloading such files onto the company network or a client machine places the company at significant risk for legal action by the copyright holder and other organizations. File-sharing networks also provide ready access to pornography or other offensive material, subjecting the company and its employees to additional legal risk.

Network disruption

While the company has significant Internet bandwidth to accommodate all business-related activity, performance can degrade significantly when P2P file-sharing applications are used, especially when large files are being downloaded. This problem is compounded when other users on the P2P network use company bandwidth to download files from the employee's computer, which can significantly slow other services such as e-mail, Web browsing, and—more significantly—e-commerce on the company Web site.

Security

P2P networks can introduce significant gaps in an otherwise secure network. Threats such as worms and viruses can easily be introduced into the company's network. P2P applications, if modified, can also allow users outside the company to gain access to data on the employee's computer or even the corporate network. (Although most P2P applications allow users to disable file-sharing, such measures do little to prevent threats from being downloaded onto a user's machine.) Some P2P applications will also allow third parties to see the user's IP address. The use of so-called spyware, which can allow network users to see your Internet browsing or can harness the use of your machine's resources, is also common on many P2P applications.

Protecting the company's intellectual property

The use of P2P file-sharing applications can sometimes allow other members of the P2P network to have access to everything on your local machine, putting the company's intellectual property assets, as well as an employee's personal information, at risk.

Copyright ©2003 CNET Networks, Inc. All rights reserved.

To see more downloads and get your free TechRepublic membership, please visit www.techrepublic.com/downloads.