

A CORPORATE POLICY GUIDE TO
COPYRIGHT USE AND SECURITY ON THE INTERNET



AN OPEN LETTER TO AMERICA'S CORPORATE LEADERS

As with any business, the people and companies that create music, movies and other copyrighted material rely on getting a fair reward for their creativity, time and hard work. That happens when people buy these works, but not when they steal them—including by copying or transmitting them without the permission of the copyright owners.

Unfortunately, employees of companies and other organizations sometimes use their employers' computer systems to engage in unauthorized copying of music, movies and other copyrighted material. This activity not only wastes the organization's time and system resources, but it is also **illegal**. Such activities on your systems can put your organization at legal risk, tarnish your organization's reputation and increase security risks for your computer systems.

This brochure explains the problem of copyright theft in the corporate and office environment, what can be done about it, and how you can implement policies to minimize the risk to your organization. Copyright theft is bad business for everyone!

Sincerely,



Hilary B. Rosen
Chairman and CEO
Recording Industry Association of America



Jack Valenti
President and CEO
Motion Picture Association of America



WHAT ARE THE RISKS?

Unauthorized copies of music, movies or other copyrighted material on your computers pose legal risks to your organization.

Music, movies and other copyrighted material is someone else's property. When your employees put music, movies, videogames or other software on your computer systems without a license or other permission from the copyright owner, it is not 'sharing' or 'fair use.' It is theft. It is copyright infringement. When these works are made available to others in your organization, or to the public over the Internet, it is no different than running an illegal distribution business.

Legal risks include injunctions, damages, costs, and possible criminal sanctions against your organization or its directors.

The laws of virtually every country impose severe civil and criminal penalties for copyright infringement, and copyright owners regularly and successfully take legal action against organizations whose computer systems are used for copyright infringement.

As the software industry has done for years, the music industry has started to identify organizations whose computer systems are used to upload, download and store or transmit music in MP3 or other formats without authorization. Such violations will be prosecuted. For example, in April 2002, the recording industry entered into a \$1 million settlement with Integrated Information Systems, Inc., an Arizona-based high-tech company whose employees accessed and distributed thousands of infringing music files using the company's server.

Illicit copying or transmission of music, movies or other copyrighted material also raises security and other risks for your computers and networks.

- **Viruses, Trojan horses, and other harmful code.** Unauthorized files purporting to be music or other copyrighted material may not be what they claim. They may harbor rogue programs, links or scripts that pose a risk of damage to your systems.
- **Spyware.** Peer-to-peer software often includes undocumented 'spyware' that reports on computer usage, delivers advertising and other unsolicited files or allows others to tap into your computer resources. Spyware can be difficult to remove without investing substantial time, and in some cases, can cause computer damage.
- **Exposing Private Files.** Peer-to-peer software frequently is configured so that users are able to search and download not only files containing music and other copyrighted material, but also other files – like those containing your confidential business information.
- **Firewall breaches.** Peer-to-peer software may demand an open port in your firewall or otherwise make your networks susceptible to attacks by hackers.

Illegal downloading and distribution of copyrighted material consumes your computer system resources and distracts your employees from doing their jobs.

You provide your employees access to computer systems and the Internet, and pay them, so that they will do their jobs. When they surf the Internet, illegally download files, and make those files available over the Internet, they can eat up gigabytes of your storage media space, consume your network and Internet bandwidth, and increase demands on your IT department. They also are not spending time doing their jobs. You become a victim of piracy, too!

WHAT CAN BE DONE?

Set a clear policy against copyright theft.

Users, managers and IT personnel need to understand that the unauthorized copying or transmission of someone else's music, movies or other work is copyright theft, which the company does not condone.

This is best communicated in your organization's **policy manual** or **employee handbook**. For a sample memorandum to employees and policy statement, see pages 4 & 5.

Audit your systems for unauthorized copyrighted material.

Many organizations already do regular audits of their systems for certain types of unauthorized copyrighted material, such as software that has not been properly licensed. A number of companies offer services to audit your network (and all connected devices such as desktops, laptops, etc.) and watch for the unauthorized reproduction or distribution of copyrighted material. Audits should include **all major types of copyrighted material, including music and movies**.

For example, music files typically are stored on computers in .mp3, .wma or .wav format. A typical compressed commercial recording takes up 3-5 megabytes, and is often found in a **\\my music** or **\\shared directory**.

For a list of some of the Corporate Network Management companies that offer services to protect corporate networks from unauthorized use of copyrighted materials, visit: www.copyrightassembly.org, www.mpaa.org, www.musicunited.org, www.riaa.com.

Delete all unauthorized copies of copyrighted material.

Commercial recordings of music and movies are virtually never licensed for copying other than for: use in a media or entertainment business, or for Internet distribution through recognized, legitimate online services.

Unless a user produces a license or subscription agreement from a legitimate music or movie service, you should assume that copies of music and movies on your computers are illicit. There are no excuses such as 'fair use' for corporate or Internet copying of these works without the permission of the copyright owner.

Take security precautions against further violations.

Organizations can take technical precautions to reduce the risk of unauthorized copying of copyrighted material. These include:

- **Firewall configuration.** Your corporate Internet firewall can be configured to screen out infringing files and illicit services.
- **Port scanning.** Software is available that detects attempts to use a peer-to-peer file transfer service.
- **Virus protection.** Up-to-date anti-virus software can screen out rogue files such as viruses and spyware.
- **Automatic audit/inventories.** Software is available for maintaining a rolling inventory of installed applications and files.

Designate a copyright compliance officer.

Someone within your organization should be responsible for protecting you against copyright theft on your systems. In many organizations, the IT or finance director is given this responsibility.

The person needs to be sufficiently senior to insist upon ongoing compliance with your organization's policy, to take prompt action to remove illicit material, and to deal with disciplinary actions and other issues that may arise.

SAMPLE MEMO TO EMPLOYEES

MEMO

TO: (Distribution list)
FROM: (Senior Officer)
SUBJECT: Policy on Use of Copyrighted Material
DATE: (Insert)

The purpose of this memorandum is to remind you of (Organization's) policy on the use of copyrighted material on (Organization's) computer systems and networks.

Unauthorized copying, distribution and certain other use of copyrighted material is illegal and can expose you and (Organization) to severe civil and criminal liability under the copyright law. This applies to all types of copyrighted works, including music, movies, software and other literary and artistic works.

Employees must not make, store, transmit or make available unauthorized copies of copyrighted material using (Organization's) computers, networks or storage media. Nor may employees use peer-to-peer file transfer services or take other actions likely to promote or lead to copyright infringement. If you have stored unauthorized copies of music, movies, software or other copyrighted works on (Organization's) computer systems, you should delete those copies promptly.

(Organization's) complete policy on the use of copyrighted material is attached. Please note that employees are subject to disciplinary action, including possible termination, for violation of this policy. (Compliance Officer) will be organizing regular audits of (Organization's) computers and networks to ensure compliance and, if necessary, will remove unauthorized copies if you have not done so.

Please do not hesitate to contact (Compliance Officer) if you have any questions.

POLICY ON THE USE OF COPYRIGHTED MATERIAL ON (ORGANIZATION'S) COMPUTER SYSTEMS AND NETWORKS.

1. (Organization) respects the copyrights of those involved in creating and distributing copyrighted material, including music, movies, software, and other literary and artistic works. It is the policy of (Organization) to comply with copyright law.
2. (Organization) provides its employees access to computer systems and the Internet to allow them to do their jobs on behalf of (Organization). Employees shall [use (Organization) computer systems and networks solely for business purposes] [make no more than insubstantial use of (Organization) computer systems and networks for personal purposes].
3. When (Organization) employees need to use copyrighted materials to do their jobs, (Organization) acquires appropriate licenses.
4. (Organization) employees shall not store or otherwise make unauthorized copies of copyrighted material on or using (Organization) computer systems, networks or storage media.
5. (Organization) employees shall not download, upload, transmit, make available or otherwise distribute copyrighted material without authorization using (Organization's) computer systems, networks, Internet access or storage media.
6. (Organization) employees shall not use or operate any unlicensed peer-to-peer file transfer service using (Organization's) computer systems or networks or take other actions likely to promote or lead to copyright infringement.
7. (Compliance Officer) is responsible for carrying out this policy. Questions concerning whether an employee properly may copy or otherwise use copyrighted material should be raised with (Compliance Officer or the legal department) before proceeding.
8. (Organization) reserves the right to monitor its computer systems, networks and storage media for compliance with this policy, at any time, without notice, and with or without cause.
9. (Organization) reserves the right to delete from its computer systems and storage media, or restrict access to, any seemingly unauthorized copies of copyrighted materials it may find, at any time and without notice.
10. (Organization) employees who violate this policy are subject to discipline as appropriate under the circumstances. Such discipline may include termination.

Recording Industry Association of America

1330 Connecticut Avenue, NW

Suite 300

Washington, DC 20036

202.775.0101 (phone)

202.775.7253 (fax)

www.riaa.com

Motion Picture Association of America

1600 Eye Street, NW

Washington, DC 20006

202.293.1966 (phone)

www.mpa.org

High Speed

Transition

Download