Appropriate Internet Use

Goals: ***This session should help the participant:***

- Understand the potential problems involved in employee use of the Internet at work.
- Develop a reasonable and effective policy to prevent inappropriate use.
- Enforce the Internet use policy properly, balancing employer and employee interests.

1. Realize the Potential Problems Involved in Employee Use of the Internet

- The Internet is an essential business tool for most organizations today.
  - –It not only provides instant access to vital information, it also offers instant communication anywhere in the world at any time of day.
- Access to the Internet allows employees to carry out important work-related duties.
- But the Internet also provides employees access to inappropriate information and opportunities inconsistent with business needs that may be harmful to your organization.
- Employee abuse of the Internet on the job can:
  - –Raise critical security issues (e.g., expose networks to viruses, give hackers an easy way in to your computer systems, and allow unauthorized people access to confidential information)
  - –Make you vulnerable to lawsuits (employers have been sued by employees for sexual harassment when co-workers use the Internet to access pornography, for example)
  - –Reduce productivity (e.g., when employees spend time on pursuits such as online shopping and banking, trading stocks, checking sports scores, reading online newspapers, gambling)

2. Understand Your Legal Rights to Control Internet Use

- The Electronic Communications Privacy Act allows you to control employees' Internet use on computer systems owned and operated by the organization.
- Courts generally hold that you have a legitimate business interest in maintaining computer security and preventing inappropriate use of computer systems, and this includes Internet use.
- Your right to control Internet use should be backed up by a policy that spells out the rules and has been properly communicated to employees.
- Have your attorneys review your Internet use policy and enforcement programs.

3. Make Sure You Have a Well-Publicized Internet Use Policy

- Your Internet use policy should be in writing and included in your employee handbook.
- The policy should clearly define appropriate and inappropriate Internet use in the workplace.
  - –If you decide to use filtering software to block certain websites, inform employees.
- Be sure to state in your policy that computer systems, including all tools and information accessed from the organization's systems, are the organization's property and that employees should have no expectation of privacy when using the organization's computer systems.
- Your policy statement should also warn employees that if they violate the rules, they will be subject to discipline up to and including termination, as well as possible legal action.

- Your policy must be supported by formal employee training in computer system use rules (including during orientation of new employees) and by regular reminders about the rules.

4. *Enforce Your Policy Firmly and Consistently*

- Having a policy is not enough; you must also enforce the policy and discipline offenders.
- Many organizations use software and other tools to monitor Internet use and enforce rules.
  - –Monitoring software can provide lists of websites and even give you the ability to search an employee's Internet file by keywords (e.g., sexually explicit or gambling-related words).
- Some organizations monitor all employee computer use, while others monitor randomly.
  - –Some only monitor if there is an indication that an employee might be abusing the system.
- Whichever approach you choose, let workers know that they are being (or may be) monitored.

5. *Develop a Reasonable and Balanced Approach to Internet Use*

- Surveys indicate that in most workplaces today, employers and employees agree that some nonbusiness use of the Internet is both inevitable and acceptable.
- When allowed, appropriate personal use of the Internet in the workplace should be clearly understood not as a right, but as a privilege–a privilege that can be revoked if abused.
- Your policy might, for example, allow employees to access their personal e-mail during the day and use the Internet briefly for personal banking, checking sports scores, etc.
  - –Specifically limit the occasions when personal use of the Internet is permitted (for example, on scheduled work breaks only), and place a limit on the amount of time employees can spend this way (for example, a maximum of 15 minutes per workday).
- This kind of approach is probably similar to the approach you take with other nonbusiness activities employees engage in, such as personal telephone calls, reading newspapers, etc.
  - –A certain amount of this type of activity is expected and can generally be tolerated as long as the privilege isn't abused and employees' work isn't affected by excessive time wasting.
- Most employers prefer to focus on the serious issues involved in employee Internet use (e.g., security, downloading of offensive material, gambling) and allow a certain amount of inoffensive use as long as it doesn't get out of hand.

Applicable Regulations: Electronic Communications Privacy Act

Training Tips:

- Review your organization's Internet and e-mail use policies.
- Explain what, if any, nonbusiness use of the Internet is acceptable for your employees.
- Ask participants to discuss any problems they have had with employee use of the Internet.

Knowledge Review:

–Distribute copies of the handout and discuss the Internet policy pointers. Then have participants complete the Appropriate Internet Use Quiz. It provides a useful review of the subject.