The Trusted PROFESSIONAL

io.8 • August 2001 The Monthly Newspaper of the New York State Society of Certified Public Accountants www.nysscpa.org

management matters

Moving Toward a Company Policy on Electronic Communications

By *Jonathan A. Wexler*

As employers become aware of the potential for abuse of their electronic communication system, more and more are monitoring e-mail and Internet usage by their employees. An American Management Association survey released in April 2000 found that 38 percent of surveyed employers store and review employee e-mail messages and 54 percent monitor Internet usage. The same survey revealed that 16 percent of the firms have discharged employees for misuse or personal use of their e-mail or Internet systems. Monitoring, or at least the right to monitor, is an essential part of any electronic communication policy, and it is legal, with certain caveats.

The 1986 federal Electronic Communications Privacy Act prohibits the unlawful interception of electronic communications, including e-mail, and prohibits the unlawful access to such communications while they are in electronic storage. However, exceptions in the statute [illegible] substantial latitude to monitor of the computer system that interferes with any employee's work duties or compromises the effectiveness of the system should be prohibited. Use in furtherance of an employee's personal business should be disallowed. However, employers should be aware that allowing reasonable personal use means that employers cannot prohibit reasonable use that involves union organizing and activities.

Rule 3: Eliminate an expectation of privacy. Employees should be told that the employer can and will intercept and monitor e-mail communications and Internet usage to the extent necessary to protect its business interests, and that usage of these resources constitutes employee consent to monitoring. Some experts believe the employer should describe the circumstances under which monitoring will occur, but the more restrictions the employer places on itself, the more likely there could be litigation concerning subsequent monitoring.

Rule 4: The policy should prohibit the use of the system to browse, retrieve, display, or send any offensive, inflammatory, or obscene language or images, including sexually explicit material.

Rule 5: Employees should be told to treat e-mail the same as any other form of communication in the workplace. The policy should prohibit the use of the system in any manner that reasonably might cause another to feel offended, embarrassed, or harassed, including any personal attacks or any pejorative or offensive material based on race, religion, national origin, age, sex, sexual preference, or disability.

Rule 6: The policy should prohibit e-mail or computer usage that is intended to mask or misrepresent the sender or user. Employees shall not use anyone else's password, or use encryption software not provided by the company. Employees should be told that they must disclose their passwords upon management request.

Rule 7: The policy should prohibit employees from retrieving or downloading copyrighted material or software and, conversely, from sending any confidential information or trade secrets via e-mail or over the Internet without management approval. Additional instruction may be appropriate to avoid computer viruses.

For a basic model policy, see the accompanying exhibit.

The creation and dissemination of a policy governing the use of a company's electronic communication systems can effectively control the misuse of those systems and reduce potential company liability that can result. ▶

Jonathan A. Wexler, Esq., is an attorney in the New York office of Vedder Price Kaufman & Kammholz, where he practices labor and employment law.