Bodyguard for Electronic Information

HR Magazine Vol. 55 No. 1

Protect electronic information with a current policy.

1/1/2010 By Nicole Kamm

Imagine a business operating without any locks on its doors. As preposterous as that sounds, some companies operate without the equivalent of locks on their electronic information—a current electronic information policy.

That can be a costly mistake in today's workplace, where most companies' operations depend on computers and the ways electronic information can be compromised are manifold.

Employees' misuse of computers includes hours spent surfing the Internet, sometimes visiting social networking sites for personal reasons or even pornographic sites. As a result, employers face risk of contamination from viruses, inefficiency and online threats to the corporate brand. And, employers that discipline or terminate employees may learn the hard way that computer misuse includes tampering with and even deleting key data.

An employer's first line of protection is a current, clearly worded, readily available computer and Internet use policy. As changes in electronic information multiply, so do employers' compliance obligations. Hence, such policies come with built-in obsolescence; last year's policy won't do.

Consider how dramatically electronic information was transformed in 2009 by the rapid spread of social networking and micro-blogging. The new year may bring just as far-reaching changes. Even HR professionals who help information technology (IT) and legal executives revise and update electronic information policies early in 2010 should revive that resolution as needed, possibly several times a year.

Yearly updates aren't mandated by law, but they are worth the effort. Current policies will reduce legal risk and enhance your organization's reputation as a fair employer.

Policy development should go with regular training. Employees should know what constitutes a violation, what the potential disciplinary actions are and why safeguards are necessary. They also should be told that compliance is mandatory, without exception.

Set the Boundaries

Make sure your policy has the basics. Any electronic information policy should:

- Define expectations regarding computer use.
- Delineate rules governing data storage and distribution, the use of company e-mail and other electronic systems—including pagers, cell phones and personal digital assistants.
- State what confidentiality, if any, employees can expect to maintain.

Employees should be reminded that their electronic systems are company property used for business only. To the extent employees use computers, cell phones and pagers for personal use, they should have no expectation of privacy.

An effective policy explicitly establishes company ownership of computers, networks, servers, files, e-mails, phones and text-messaging devices. Establishing ownership reduces privacy expectations and strengthens the employer's rights.

Acceptable and unacceptable uses of company property should be clearly defined. Describe what kinds of language, material and images employees are permitted to access and transmit. Employees must understand and acknowledge that the employer can and will use the company's computer system to monitor all activity.

To prevent data tampering or removal, make sure policies are broad and restrict downloading and storage of sensitive data or software on employee-owned devices, and on employer-owned devices without written approval. Encryption and firewall software can prevent unauthorized downloading. In addition, software is available that limits the devices plugged into Universal Serial Bus ports to further block illicit use.

Virus Prevention

Creating and disseminating an electronic information policy informs employees about restrictions on their use of technology at work. It also supports disciplinary action should an employee misuse company property and defends such an action that is subsequently challenged in court, as was the case when I represented a hospital in a wrongful termination lawsuit.

Prior to the plaintiff's termination, the hospital's IT director discovered a computer virus on the computer system. He promptly conducted an investigation to determine the source. The investigation revealed that the virus was introduced through a computer connected to the Internet in the emergency room (ER) admitting department, where the plaintiff worked.

As part of the investigation, the IT director reviewed the web sites visited by employees in the ER admitting department. He discovered that some employees, including the plaintiff, had been using the Internet in violation of the hospital's Internet policy. The employees knew about the policy and had previously acknowledged receiving it. On the day the virus entered the computer system, according to the IT director's investigation, the plaintiff had spent more than seven hours of her eight-hour shift on the Internet, visiting hundreds of web sites for purposes unrelated to her professional duties. As a result, the plaintiff and two other employees were terminated.

At mediation, I presented the hospital's comprehensive computer and Internet use policy alongside a detailed spreadsheet that charted both the time, minute by minute, that the plaintiff had been on the Internet for nonwork purposes that day and the web sites she had visited. The result: Case dismissed.

Monitoring Employees

As in the above case, monitoring controls, supported by policies, are an effective method of protecting property and preventing security violations.

There are several strategies for monitoring computers and other devices. Software enables employers to track server, e-mail and Internet activity as well as to gather information directly from computers and to conduct forensic analyses. Software also can restrict access to certain Internet sites. Most of this software can be installed without alerting users.

"Keystroke monitoring" tells how many keystrokes each employee makes per hour. It can inform employers if employees go beyond or fall below the expected number of keystrokes required to fulfill their responsibilities and may raise red flags as to what employees are doing other than assigned tasks.

Another technique allows employers to track time spent away from computers or idle time on computers. Other tools screen for select words, phrases or images. Monitoring can be outsourced to a third party.

Employers, however, should be aware that employees may be given some protection under certain circumstances. For example, union contracts may limit an employer's right to monitor. Public-sector employees may have some additional rights under the Fourth Amendment, protecting against unreasonable government search and seizure.

Courts have suggested that reasonableness is a standard for determining acceptable monitoring practices. Electronic monitoring is generally reasonable where there is a legitimate business purpose, where policies exist to set the privacy expectations of employees, and where employees are informed of the rules and understand the methods used to monitor the workplace.

Often, though, employers do not take steps to monitor employees. Instead, employees seem to be closely monitoring employers.

For example, in 2008 an employee at a Florida architecture firm saw a help-wanted ad in the newspaper for a position that looked suspiciously like her current job, and with her boss' phone number listed. The

woman assumed she was about to be fired. She went to her office and erased seven years' worth of drawings and blueprints, worth an estimated $2.5 million.

It didn't take long for the employer to discover the responsible party. The woman was the only other person who had full access to the files. Police arrested her and charged her with causing greater than $1,000 damage to computer files, a felony. Her boss was able to recover most of the files, but only after using an expensive data recovery service. And the woman had not been in danger of being fired: The ad was for the owner's wife's company.

Tight Controls

Layoffs are regrettable yet often inevitable byproducts of difficult economic times. When an employer decides to terminate an employee, the discharged employee's continued access to confidential information is a critical consideration.

Upon notice of termination or after an employee's last day, the employer should immediately terminate the employee's access to the offices, computers and computer system, including remote access and BlackBerry service, voice mail, e-mail, and client and company documents. If the employee requests computer access to retrieve personal information, the employer should have either a company representative do it or monitor the employee.

In some cases, particularly where wrongdoing is suspected or there is increased risk of litigation, the employer should preserve the employee's hard drive, network files, e-mails and BlackBerry.

Data loss and damage is, in large part, preventable. Business leaders should know exactly where sensitive data is, how it is used and how to prevent it from being illicitly copied or sent outside the company. Well-defined policies, clear communication, tight controls on data access and an exit procedure for departing employees are essential.

How Much Networking?

A trend in hiring is to find the applicant's profile on social networking web sites such as MySpace, Facebook, LinkedIn and Friendster. In *Moreno v. Hanford Sentinel Inc.*, 172 Cal. App. 4th 1125 (2009), regarding a matter unrelated to employment, a California Court of Appeal held that when a person posts on MySpace, it is not "private." Arguably, there is no invasion of privacy when an employer uses posted information or discloses posted information to others.

However, employers should still be careful about how they use the information they discover online. For example, an employer might learn that an employee identifies himself or herself as being part of a particular religion or having a particular sexual orientation, or some other information that falls within a protected category. If mishandled, this knowledge could lead to violations of state or federal laws.

Employers should consider whether they want to limit employee access to such sites, and specify how in their policies. If some personal use is allowed at work, it should be spelled out in clear terms. For example, "limited personal use of some sites is permissible, as long as it is consistent with conscientious job performance." Prohibited conduct, such as gambling, entertainment downloading, visiting pornographic or adult sites, and making personal purchases, should be included in any policy as well.

Keep It Real

There is little good that comes from having a computer and Internet use and monitoring policy if employers don't enforce it. Routine monitoring and enforcement of policies, and discipline for violations, are as important as the policy. Most managers are willing to live with a little personal use of computers at work and acknowledge that there are periods of unproductiveness in every workday. Ultimately, it is top executives' responsibility to determine how much personal use is too much and to identify appropriate methods to curb excessive use.

Too much leeway can be dangerous. For all you know, an employee might be accessing information, visiting an adult web site or sending an inflammatory e-mail via the company's system while you are reading this article.

The author practices employment litigation and counseling, primarily for employers, with the Encino, Calif., law firm Lewitt, Hackman, Shapiro, Marshall & Harlan.