NATIONAL LAW ENFORCEMENT AND CORRECTIONS TECHNOLOGY CENTER
A program of the National Institute of Justice

From Summer 2000 *TechBeat*

TECH b•e•a•t

Dedicated to Reporting Developments in Technology for Law Enforcement, Corrections, and Forensic Sciences

'Policing' Internet Use

According to a survey by Information Week Magazine, *40 percent of employees spend at least 1 hour a day surfing the Internet without a business purpose.*

Every day, millions of Americans log onto their computers to check e-mail, catch up on the news, and research the vast amount of information to be found in cyberspace. Many criminal justice agencies now depend on the resources and information available via the Internet and allow their personnel unrestricted access. However, this access can be abused if guidelines are not in place for its proper use.

The amount of communication effected through the Internet is growing at an amazing rate. According to Michael Overly, a lawyer with a Los Angeles firm and author of *E-Policy: A Guide to How Corporations Can Deal with the Internet,* more than 1 million messages pass through the Internet every hour. With the increasing use of the Internet by law enforcement and corrections agencies, administrators now face a new problem: how to police their own employees' use of cyberspace while on the job.

"It is especially important for public entities to manage their Internet resources properly," Overly says. Public entities are subject to open records requests. These requests can cover such information as an employee's incoming and outgoing e-mail messages, records of visited and "bookmarked" Internet sites, and downloaded files saved to an employee's computer or the agency's network.

So, how much control should a department have over Internet access by employees and how much privacy are employees entitled while they conduct business on the Internet?

Overly recommends that the best solution is to adopt a clear, concise Internet use policy so that the department can reduce the potential liability to employees and those outside the agency as well as protect confidential information and reduce the waste of the agency's computer resources. "If employees are downloading large files and storing them on their drive," Overly says, "it can affect the functionality of the entire system."

When developing a policy, a few critical areas must be addressed. Overly recommends that:

- The agency educates personnel regarding privacy issues, reiterating that anything made available through the Internet can be read and viewed by other parties.
- Employees receive instruction on how they can maintain confidentiality in their Internet communications.
- The agency develops a concise statement of what an employee can and cannot do while on the Internet, including who has ownership of downloaded and stored files. "It's important that an employee knows that all computer Internet files or documents on the hard drive belong to the agency," Overly says.
- The agency has a statement that a violation of the policy by an employee can lead to discipline or termination. All employees of the agency should sign and date a copy of the policy.

Overly says a good policy might begin with the following statement: "Our computer and Internet e-mail system is to be used to assist you in your job. However, you may use the system for incidental personal use, provided that your use does not impact your job function, other employees around you, or materially impact the operation of the computer system."

Chief Walt Vanatta of Colorado's Craig Police Department implemented a department-wide Internet use policy at the beginning of 1999. "We had some instances where we had problems with downloaded files that contained viruses or were too large for our system," Vanatta says. "I also wanted to address personal Web sites that were created by employees. Some of them made it look like the department endorsed the site."

Before penning his current policy, Vanatta gathered samples of similar policies from departments across the United States. He also incorporated an already existing city policy on the same issue. "Don't recreate the wheel,"

he says. “Modify various policies so that it will meet your purposes.”

Overly adds, “It takes very little to put these policies into place. In the long run, the amount of time and money saved in potential lawsuits is well worth the effort.”

For a copy of the Craig, Colorado, Police Department Internet use policy, e-mail Chief Walt Vanatta at wvanatta@ci.craig.co.us or access the document through the International Association of Chiefs of Police Web site, www.theiacp.org/.

This article was reprinted from the Summer 2000 edition of *TechBeat,* the award-winning quarterly newsmagazine of the National Law Enforcement and Corrections Technology Center system, a program of the National Institute of Justice under Cooperative Agreement #96–MU–MU–K011, awarded by the U.S. Department of Justice.