



Guest column: Don't destroy records of former workers

March 2, 2010

An employee has left your company, so you've cleaned out their work space, their files have been thrown away and their computer hard drive is wiped clean. Now you just have to prepare for the new employee to arrive, right?

Not so fast. You also need to be concerned about what you may have needed from the past employee's records — the very records that you just disposed.

Companies still are responsible for information even after the employee is no longer there. You never know when you may need past employee files during an audit or even in the event of litigation, so developing a policy to address their retention and destruction is crucial.

Begin by assessing the following areas before doing a mass file purge:

- **E-mails:** Legal regulations have been enacted that treat an e-mail message just like any other record. The e-mails you keep from the past employee will really depend on your industry, but consider keeping e-mails that reflect the position of your business, complete a transaction or are part of an official record.
- **Hard drives and shared drives:** Be sure to go through hard drives before wiping the computer clean. Also, check any shared drives as well, as these files may be different than those on the hard drive.
- **Content and document management systems:** If your company has a system that manages and retains records through a secure Web site, don't forget to look at the files stored here. You'll especially want to do this if a new employee will have remote access to this information.
- **Hard copy files:** In addition to retaining certain electronic files and e-mails, be sure to go through other hard copy records that the employee may have had, including blueprints, maps, magnetic media and mail. There are numerous state and federal

regulations regarding retention periods for different file types — typically one to three years. Consult your company's legal, accounting and records management professionals to determine exactly what should be kept for your situation. Keep in mind that retaining everything forever isn't a good idea as federal law states that during an audit, all records on hand can be looked through, and that's regardless of whether it's a current or former employee. When it comes to destruction of past employee files your company no longer needs, in order to protect both your company and past employee from falling victim to identity theft, be sure to shred everything. Developing a policy that addresses retention and destruction of past personnel files will take some time up front, but you'll sleep a lot better knowing you're protecting your business and past employees' information from getting into the wrong hands. Eric Haas is president of Automated Records Management Systems, a full-service commercial records center in De Pere.

Advertisement



hp HIT PRINT AFFORDABLY

Have you HEARD THE BUZZ?

Save \$50 WHEN YOU TRADE IN YOUR OLD PRINTER.

OFFICEJET PRO DELIVERS 50% LESS COST-PER-PAGE THAN LASER.

LEARN MORE AT HP.COM/OFFICEJETPRO

Print Powered By FormatDynamics™