Tis the Season…..

The holidays have come and gone and it's time to start the new year. What does that mean for your practice? Well, if you haven't reviewed your basic technology policies in a while, now would be a good time to put this project on the 2012 to-do list. To help you get organized and informed on these essential policies and procedures, here is a reprint of an excellent article by Sharon D. Nelson and John W. Simek of Sensei Enterprises. *— Wendy Inge, Virginia risk manager for Liability ALPS*

Essential Law Firm Technology Policies and Plans

by Sharon D. Nelson and John W. Simek

Technology users run amok. They are rogues, far more apt to do what they please than to do what their employers dictate. Sometimes law firms try to control their employees with technology. Our favorite example is using technology to ban visits to social media sites. Employees, after complaining bitterly about their bosses, will simply use their smartphones and go wherever they want on the Web.

Policies that have a dose of common sense can often accomplish more than technology.

Law firms also need plans. What if your firm is sued and you find yourself under a litigation hold? Do you know what needs doing and who will do it? What if a major earthquake or flood hits and you are suddenly without an office? In a modern day nightmare, what happens if you find out that someone has hacked into your law firm servers? What's the plan Stan?

We could write an article on each of the policies we've listed below, but space demanded a condensed version to get you thinking about whether you should be developing policies you don't have or reviewing those you do have to see if they need updating. Remember, there are a lot more policies and plans that law firms should have — these are specifically related to technology.

And for heaven's sake, TRAIN, TRAIN, TRAIN at least once a year. No one remembers the fine points of plans and policies without annual memory refreshers and the technology updates will necessitate minor changes at a minimum.

Electronic Communications and Internet Use Policy

Don't blame the employees if you haven't been clear about what they can and can't do. Most employers allow incidental use of email and Web surfing for personal purposes and that seems fair enough to us. But if an employee is engaged in personal Web cruising or electronic communications for the bulk of their day, they are outside the policy.

You may want to forbid streaming at work (audio and video), which hogs bandwidth and can slow your network. Forbid downloading executable files without checking with IT — who knows what malware may ride in on those files?

Typically, users are forbidden to visit sexual sites, "hate" sites or sites involving illegal activity, such as gambling sites. When visiting interactive sites, they are generally encouraged to think twice before using the firm name in any manner. Privacy and confidentiality are always addressed.

A toothless policy won't work. If you are going to make rules, you need to be able to monitor conduct, at least periodically, and to punish infractions. This is true for all policies, so be prepared to police your policies once they are implemented.

If you've no idea where to start, here's one model policy: http://apps.americanbar.org/buslaw/blt/ndpolicy1.html.

Social Media Policy

You might think this would fall under the policy above, but most businesses have a separate social media policy — in part, because social media has been a world in which the Indians run the reservation while the chiefs are helplessly wringing their hands.

Forbidding the use of social media doesn't work. It not only irks the employees but they ignore the prohibition. If you have technology enforcing the prohibition, they will use their smartphones or other personal communication device.

By way of contract, large businesses are generally embracing social media — at one general counsels meeting in New York, we heard the general counsels of Sprint and Coca-Cola® happily laud their employees as "social media ninjas." They go out and spread the gospel on behalf of the companies. Of course, in law firms, we have to be mindful of our ethical rules — but within those rules, one can do a lot of good for the firm.

So, follow the KISS principle and keep the policy simple. No obscenities, no discriminatory postings, no angry postings, proof before you post, don't give legal advice, remember that social media lives forever, speak politely to everyone you interact with and report problems to a supervisor. To keep from reinventing the wheel, you can find a sample social media policy at http://thebyrneblog.files.wordpress.com/2010/03/sample-social-media-policy.pdf.

Document Retention Policy

If only law firms would learn to take out the digital trash. Instead, they tend to move all their data when they perform a technology upgrade because storage is so cheap. What is NOT cheap is searching through all sorts of useless data either when looking for client documents or searching the data in response to a discovery request in a lawsuit.

You really don't need the twenty-five emails it took to schedule one meeting. But lawyers tend to keep it all. The first rule of creating a document retention policy (DPR) is simple: If you are governed by federal or state law or regu-

Risk Management continued on page 64

Risk Management continued from page 64

need to cease automated janitorial functions on your network. Periodic litigation hold notices must be sent out. And that's just the beginning. Further fodder for thought may be found at http://tamut.edu/recordreten/Sample%20Litigation%20Hold%20Procedures.pdf.

Though column space doesn't allow us to delve extensively into the components of all of these policies, we have tried to provide a snapshot of the most common policies and plans and give you a link to further resources. These policies and plans are an integral part of risk management and ensuring business continuity, two things near and dear to the heart of all lawyers.

The authors are the president and vice president of Sensei Enterprises, Inc., a legal technology, information security and computer forensics firm based in Fairfax, VA.
(703) 359-0700, www.senseient.com