Essential Law Firm Technology Policies and Plans

By Sharon D. Nelson, Esq. 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 e-mail 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 really slow down 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 do 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 25 e-mails it took to schedule one meeting. But lawyers tend to keep it all. The first rule of creating a document retention policy (DRP) is simple: 1) If you are governed by federal/state law or regulations, follow them! If federal and state requirements

conflict, obviously follow the more stringent requirements. The second rule is equally simple: 2) If you are governed by internal by-laws, other mandatory procedures, or industry standards, abide by them. Now comes the dicey part. Rule #3: If you are on your own after following rules 1 and 2, assume all the documents in your possession, paper and electronic, will be the subject of a lawsuit somewhere down the line. What is best kept and what is best thrown away? Drafting these policies is no walk in the park. It requires more intensive thought than might appear at first blush. Will it help or hurt you to keep successive drafts of documents? The deeper you delve into policy formation, the more niggling issues tend to pop up. Don't expect to formulate a sound DRP overnight. You can find a sample DRP at http://apps.americanbar.org/lpm/lpt/articles/ftr07046.html.

Secure Password Policy

Only the largest law firms tend to have a secure password policy and this is a shame. This is an easy one to compose now that the Georgia Institute of Technology has proven that any eight character password can be cracked in about two hours. It also proved that it takes approximately 17 years to crack a strong 12 character password. So the key rules here are simply:

1. Employees must have alphanumeric passwords of 12 or more characters
2. They must change their password at least every 30 days and cannot repeat them
3. Suggest the use of passphrases (IclimbedEverestin2000!) and prohibit storing passwords on computers or on sticky notes – though storing them on an encrypted flash drive is permissible.
4. Don't reuse the password elsewhere.
5. Have both a log-in and screen saver password.

Most of the above steps can be enforced through technology. A typical Windows Group Policy can make sure that the passwords are a certain length, change frequently, are not repeated at a certain interval and are properly applied.

Incident Response Plan

This plan generally refers to some sort of security compromise, most often a data breach, though it can also cover attempted breaches, security alarms, unauthorized access by employees, etc. The big kahuna is the data breach. More and more data breaches are occurring in law firms – and 46 states plus the District of Columbia have data breach notification laws with a possible federal law looming on the horizon.

Incident response plans help to make sure you have an action checklist:

1. Verify what happened
2. Who is in charge of the investigation?
3. Solve the immediate problem (usually getting hackers out of your network) while preserving the evidence
4. Call in outside experts or use internal resources?
5. If a data breach has taken place, what steps does the law require you to take?
6. Harden your security so this particular incident can't happen again

There is, as you can imagine, far more to consider. A good starting point may be found at http://www.comptechdoc.org/independent/security/policies/incident-response-plan.html

Disaster Recovery Plan

By now, most lawyers understand what a disaster recovery plan is. Your server has had a meltdown, your building is engulfed in flames or your office is underwater. Catastrophes take many forms. We would stress that the number one problem in disaster situations is communications. Make sure your plan identifies who is in charge of what and gives alternate ways to communicate with those who have specific job functions.

Protecting lives is the first goal but then restoring business continuity is key. There are so many factors to consider that it boggles the mind. As we learned when our building had a fire and we had no access to our office for a week, no disaster recovery plan survives first contact with the enemy. Once the disaster is over, you will no doubt find that you need to revisit and revise your plan.

Ready to roll up your sleeves and get started? There is a treasure trove of resources available at http://www.americanbar.org/groups/committees/disaster/resources/resources_for_lawyers_law_firms.html.

Mobile Security Policies

Lawyer mobility has expanded so much in the last 10 years that most of us can now work from anywhere and have access to our office documents as long as we have an Internet connection. But all this connectivity means we have serious security concerns as we connect with laptops, tablets and smartphones.

It is critical that our remote connections are secure and that we transport and store confidential data in a secure manner. Would it take an epic novel to tell you how? Yes. So it is very helpful that the SANS Institute has a suite of mobile security policy templates available at http://www.sans.org/security-resources/policies/mobile.php.

Equipment Disposal Policy

It can't leave "home" with data on it. So you can't junk your computers or donate them to charity without doing a secure wipe of the data. We recommend a free product called Darik's Boot and Nuke (DBAN) which is available at http://www.dban.org/. Once again, there are terrific resources from the ABA at http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/computerdisposal.html.

Litigation Hold Plan

If you don't have one, you're asking for trouble. If you know you have been sued or are the subject of a regulatory action, or that either one is likely to occur, you are under a litigation hold and must proceed expeditiously to preserve the relevant electronically stored information (ESI). This will require a team of folks – legal, management, IT, etc – to gather quickly and take the necessary steps. You'll need to interview key players and the IT folks to locate the relevant data, decide if you have backup media that must be preserved and whether you 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 (phone) www.senseient.com