The Importance of Developing and Following Policies

There are many places to find sample policies for the following and a great resource is the SANS Institute. To see their sample policies, just go here: https://www.sans.org/security-resources/policies.

1. **Internet and Email Usage Policy**: There may be (and likely is) a big gap between what you would deem acceptable use of company internet and email and what your employees deem acceptable use of those resources. Thankfully, you can Google "internet usage policy" and find many free examples to start with.

2. **Document and Email Retention Policy**: Lawyers tend to hold onto every document and email forever and this is simply a bad policy. You can end up with so much irrelevant digital clutter that you're unable to find the things you actually need. Your policy should comply with any applicable federal or state laws, the Rule of Professional Conduct and any other relevant regulations. It's also a great idea to contact your malpractice insurer to see what they recommend (they may even have a sample policy you could start with). The ABA has a nice compilation of records and document retention resources (http://tinyurl.com/7z8ksye) and another excellent article to read on the subject is Sample Document-Destruction Policy by Megan Zavieh, 1/21/14, Lawyerist.com (see http://tinyurl.com/hrs3hxy).

3. **Secure Password Policy**:

    a. **Why You Need This**: You need a secure password policy because of the plethora password crackers that are out there.

    b. **Types of Password Hackers**: Here are the main types (there are many more):

        i. **Dictionary attack**: This attack uses a file that contains a list of words that are found in the dictionary. This mode matches different combinations of those words to crack your device open.

ii. **Brute force attack**: Apart from the dictionary words, brute force attack makes use of non-dictionary words too.

iii. **Rainbow table attack**: This attack comes along with pre-computed hashes. When user passwords are stored by a service (say www.Target.com), the raw (actual) passwords are converted into a string of random characters by complicated mathematical computations. This conversion process is called hashing. For an extremely interesting article on this technology, see Hacker Lexicon: What Is Password Hashing? by Andy Greenberg, June 8, 2016[1].

c. **Recommended Policy**: I will warn you that a really strong password security policy can be extremely annoying because most of them recommend that you change your password every 30 days, don't repeat old ones and use unique passwords for each logon. While I appreciate the value of those rules, they would drive most people batty in short order. Here are some less annoying rules that will still help ensure your passwords are secure:

- 12 Characters, Minimum: You need to choose a password that's long enough. There's no minimum password length everyone agrees on, but you should generally go for passwords that are a minimum of 12 to 14 characters in length. A longer password would be even better.

- Include Numbers, Symbols, Capital Letters, and Lower-Case Letters: Use a mix of different types of characters to make the password harder to crack.

- No Dictionary Words or Combination of Dictionary Words: Avoid obvious dictionary words and combinations of dictionary words. Any word on its own is bad. Any combination of a few words, especially if they're obvious, is also bad. For example, "Wagon" is a terrible password. "RedWagon" is also very bad.

[1] See https://www.wired.com/2016/06/hacker-lexicon-password-hashing/

- Doesn't Rely on Obvious Substitutions: Don't use common substitutions, either — for example, "RedWag0n" isn't strong just because you've replaced an o with 0.[2]

[2] See How to Create a Strong Password (and Remember It) by Chris Hoffman, 5/29/15, How-To- Geek, see http://tinyurl.com/kx6s7uf.