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. Visit their website to view sample policies.

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.

DOCUMENT AND EMAIL RETENTION POLICY

Lawyers tend to hold onto every document and email forever and this is simply a bad policy. You end up with irrelevant digital clutter, hindering your ability to find things you actually need. Your policy should comply with applicable state and federal laws, the Rule of Professional Conduct, and other relevant regulations. Your malpractice insurer likely also has recommendations, and possibly even sample policies to get you started. The ABA has a nice compilation of records and document retention resources. Two additional starting points are a handbook from the Washington State Bar and an excellent article entitled Sample Document-Destruction Policy by Megan Zavieh.

SECURE PASSWORD POLICY

WHY YOU NEED THIS

You need a secure password policy because of the plethora password crackers that are out there.

TYPES OF PASSWORD HACKERS

Here are the main types (there are many more):

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.

BRUTE FORCE ATTACK

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

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.

RECOMMENDED POLICY

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. Such rules 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 16 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.

NO OBVIOUS SUBSTITUTIONS

Don't use common substitutions, either — for example, "RedWag0n" isn't strong just because you've replaced an o with 0.[1]

[1] See How to Create a Strong Password (and Remember It) by Chris Hoffman, May 16, 2023, How-To Geek, see https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/.