

PRINCIPAL: DAVID DRAKE FCA

**HARDEN UP!** — strengthen your password policy  
(extract from *Rosh-Tech IT* e-newsletter)

Why do I need a password policy?

Security, is the simple answer. It is similar to cutting keys for the locks to your business. You use a secure key system and are very careful as to who gets a key.

When defining a password policy for your business, it is usually a compromise between not making the passwords too easy to guess, and not making them so hard to remember that users end up writing them on the side of their screen.

What are the basic password rules?

1. Never write passwords down.
2. Never send a password through email.
3. Never tell anyone your password.
4. Report any concerns of your password being compromised.
5. Don't use common acronyms, words or names as part of your password.
6. Be careful about letting someone see you type your password.

What are the basic password requirements?

1. Minimum length – six characters recommended
2. Minimum complexity – use three of the following four types of characters:-
  - (i) lowercase
  - (ii) uppercase
  - (iii) numbers
  - (iv) special characters such as !@#\$\$%^&\*(){}[]
3. Password history — can't use previous three passwords
4. Change — every 90 days.

The good news is that the above requirements can be enforced centrally from your server. Implementing these basic conditions will make large gains in IT security.

Below are interesting data from Bloomberg Businessweek on the time it takes for a hacker's computer to brute-force crack your password, based on the length and complexity of your password:-

<b>length</b>	<b>lowercase</b>	<b>+uppercase</b>	<b>+num and symbols</b>
6 characters	10 minutes	10 hours	18 days
7 characters	4 hours	23 days	4 years
8 characters	4 days	3 years	463 years
9 characters	4 months	178 years	44,530 years

Having a sensible password policy is in your business interest. The following scenarios illustrate the reasons for having a password policy:-

- many email systems are available from the web. This means if someone knows your password they can read your emails.
- if every user knows everyone else's password, and an employee leaves, all users' passwords will be known allowing easy access.
- if your password becomes known and you never change your password, your information could be accessed indefinitely and you would never know.

*Liability limited by a scheme approved under Professional Standards Legislation*