FREQUENTLY ASKED QUESTIONS ABOUT NEW PASSWORD POLICY

Q: Why change anything? What's wrong with our current policy?
The simple truth is that it's an arms race between those who would break into systems and those who try to defend them. Passwords can be guessed by a variety of methods, and much more powerful systems are available for the task than were even though probable just a few years ago. The current minimum password length for eID is no longer sufficient to provide reasonable protection, and it's time to upgrade our defenses.

Q: If you're doing this to increase security, why get rid of the requirement for special characters? Isn't a complex password stronger?
One of the primary goals of the new policy is to increase the strength of the eID password... specifically to increase resistance to guessing attacks. There are procedural methods for helping with this, including lockouts for failed attempts, but the primary properties of the password itself are its length and the size of its character set. Mathematically, it's a power function: the size of the character set raised to the power of the length of the password, or (char-set)^length. So length is a much more powerful tool. The other goal of the policy, however, is to ease some of the difficulty of using eID passwords. Excessive complexity means a password is hard to type, and that gets even worse when using mobile devices, whose small screens mean that special characters are one or two screens away from the main text-entry screen. This is another reason to choose simplicity and length: easy to type, hard to guess.

Q: I have a special system I've worked out that allows me to generate complex passwords that I can remember easily. Why do I have to change?
Many people have advocated systems to generate passwords that are complex based on special-character substitution, keyboard patterns, combining years with book titles, and the list goes on. The basic problem shared by all of these is that a short password has become a liability, no matter how complex it is. Even if it is truly random. These mnemonic schemes may have made it easier to generate memorable random-looking passwords, but they haven't helped create passwords that are actually strong enough to survive modern attack technology.

Q: Why so long? My bank lets me have a 6-character password.
Banks have a different organizational dynamic at work. On the one hand, they have to compete for external customers who have the choice of going to a competing bank which requires shorter passwords, so competitive pressure drives toward shorter passwords. At the same time, they have financial resources to solve security issues in other ways, with tighter and more effective controls limiting customer access to most internal resources. In a university environment, we both value the openness and usability of our networks AND lack funding to implement some of the more advanced and expensive security features that would "take up the slack" created by allowing short passwords. Furthermore, just because a bank allows a 6-character password doesn't necessarily mean that it's a good thing: financial institutions have come under greatly increased attack in recent years, and some are considering increasing their security requirements even if it puts them at a temporary competitive disadvantage. As an example, PayPal for several years has offered the opportunity for customers to purchase one-time password generators that create a more complicated login process in order to help prevent account compromise, in the hope that customers will come to value that level of protection.

Q: I've read that a "passphrase" contains a space. Why can't I use a space?
The space character (and a handful of other special characters) cause problems on some of CSU's back-end administrative systems. So to ease user confusion and reduce the support burden, we've decided to prohibit the use of these characters in all eID passwords. Does that mean we don't qualify as using "passphrases"? There's no one accepted definition of passphrase, though in describing the idea, some writers have used the presence of the space character to clearly delimit the difference between passwords and passphrases. The more useful definition of a passphrase is just a stringing together of several smaller words, which may or may not form any sort of grammatical structure. Use of a different

delimiter (dash, pound sign, asterisk) or no delimiter at all doesn't mean it's not a phrase. But in order to reduce confusion on this point, we're mostly referring to "passwords".

Q: How can you expect me to remember a 15-character password?
Our brain remembers an amazing amount of stuff. But the ability to remember a sequence of things, especially in the short term, is limited to a fairly small number. Asked to remember a string of nonsense letters or ideas, we generally can handle roughly seven of these things in a row with a reasonable chance of getting them all right and all in order. If we consider these things as "chunks" of information, we shouldn't design systems that force people to remember more than 5 or 6 chunks. This is where the notion of a passphrase gets its power. If, instead of memorizing a string of 10 random characters, or the Upper/lower-case and special-character substitutions for a shorter string, we can memorize a series of three or four familiar words, our chance of remembering goes up dramatically. So, considered this way, a 15-character password made of 3 or 4 words should be much easier to remember than a short, complex password.

Q: If my password is considered strong, why do I have to change it at all?
This is not a trivial question, and has been a point of argument among security professionals for years. There are two reasons that CSU chooses to require password refresh. First, a variety of security certifications require periodic resets to prove that passwords will not, on average, be able to be guessed during their lifetimes. This argument is based on the capabilities of networks and cracking technologies, as well as the policies of servers that allow online authentication. As such, it's one of several variables that can be balanced to achieve a certain level of resistance to attack. The second reason is somewhat more pragmatic: our population comes and goes, and sometimes a password can remain active for some time, allowing access to resources long beyond when the account should have become inactive. Enabling a password reset thus also represents a sanity-checking or house-cleaning measure to make sure we're expiring accounts that are no longer needed.

Q: I keep hearing that "passwords are dead." If you're increasing security, why stick with passwords instead of biometrics or multi-factor authentication?
Love them or hate them (most security professionals hate them), passwords have been with us for a long time and won't be going away any time soon. For some higher-security applications, we do use a variety of other approaches on a small scale. Larger-scale deployment of alternative authentication measures is still expensive, and support often varies among hardware platforms and operating systems. This particular policy is aimed at shoring up "the devil we know", but we're always looking for ways to improve both the usability and the security of our information systems.