Password Instructions

How to choose, *and remember*, a secure password

This document is adapted from the password advice of respected security and cryptography expert Bruce Schneier, advice from former physicist and web cartoonist Randall Munroe, the password policy of Stanford University, and award winning security reporting by Dan Goodin of website Ars Technica. These four sources do not agree on all points. Schneier feels that Munroe and Stanford's advice is now outdated because of advances in cracking technology and processing speed. Goodin reports how proliferation of password-based services makes remembering all of your unique, strong passwords literally impossible. CCHP believes that a good password is better than a weak one or none at all and still better than a great password that you forget and write down on your monitor.

If you can use a secure password manager with truly random passwords, that is still the best option. We recommend Schneier's own Password Safe or Keepass.

Creating Passwords

DO

The best encryption in the world is useless without a **good password**.

Use the **longest** password a system will allow, *that you can remember*.

When you have a choice, use a password **at least 12** characters long, but longer is better.

Use as **many types of characters** (upper, lower, digits, letters, punctuation, spaces, symbols) as a system will allow and *that you can remember*.

Use **multifactor authentication** whenever it's available.

If you use dictionary words, make them **meaningful only to you and use more than 4 words**.

Long meaningless acronyms (of unique meaningful memorable sentences) are another good option!
`Lma(o1m2s)aago!`

DON'T

Do **NOT reuse** passwords. Trivial variations (like changing a digit at the end) are still reuse.

Do **NOT** use phrases from **popular culture or literature**. If it can be found on Wikipedia, Google Books, [Rap]Genius, the Internet Movie Database, or YouTube (*etc.*), it can be cracked automatically.

A password you **share** with anyone not following ALL of these rules– *and then don't immediately change* –**is useless**.

Remembering Passwords

DO

It's a really good idea to use a **secure password manager** to avoid the limits of your own memory and lost pieces of paper. These also allow you to use truly random passwords.

It is OK to write down your passwords (or, better, just hints) on **paper *only if you secure that paper***.

DON'T

A password you **forget or don't use is useless**.

Do **NOT** make a **text file or Word doc** on your computer with your passwords.

Do **NOT** stick your password on **a note on your monitor**.

Do **NOT email** passwords.