How do I Create a Good Password?

**NOTE:** This document is intended as a set of guidelines for creating secure passwords. Please see the Haas Technology Solutions Service Level Agreements (SLA) for basic password requirements for Students, Staff, and Faculty/PhD Candidates. In addition to the requirements in the SLA, the following paragraphs describe best practices for password creation:

Many web portals and programs require passwords with varying restrictions but here are a few tips which could assist you in formulating strong passwords for a wide variety of applications.

Passwords should not be based on known words (in any language) or words generally associated with its user (including the user's name, address, pet's name, etc.). Also avoid using all-numeric passwords as these may be easier to hack. Creating a combination of alphanumeric and special characters is best.

Most systems will accept passwords longer than 8 characters but many will ignore the characters after the eighth one. So when judging the strength of a password, think of only the first eight characters. For example, "password!" is equivalent to "password" -- a very weak password--on most systems.

Here are the basics of creating a strong password:

**DO**
- All passwords must be at least nine characters in length. However, you can strengthen your password, depending on the operating system, by increasing it to:
  - (UNIX) nine characters in length
  - (Windows) fourteen characters in length.
- Passwords must contain a minimum of one character from at least three of the following four character types:
  - Upper case letters
  - Lower case letters
  - Numbers
  - Special characters

**TIP:** To make your password easy to recall, try composing a phrase which utilizes a combination of the above characters. For example, “GoneToSchool” could be regenerated as: “g0ne+05ch001”
DO NOT

- A password should **NOT** be derivable from the user’s information such as:
  - Full name or nickname
  - Account or login name
  - CalNet directory information
  - Active Directory Information
  - Phone number
  - Addresses
  - Any information which may be associated with the user (e.g. “ClassPrez”)

- A password should **NOT** match or resemble any word found in any dictionary or list of words
- A password should **NOT** be based on:
  - Modifying any part of your name initials
  - Modifying a dictionary word
  - Popular acronyms
- A password should **NOT** use a word with a single number or character before or after it. (i.e. “berkeley!” is not a good password)
- A password should **NOT** use a simple word with just one capital letter. (i.e. Gobears is not a good password)
- A password should **NOT** be reused. Passwords should be changed regularly (annually or semi-annually) and past passwords should not be reused.