

Follow the guidelines below when creating passwords.

### **Do's**

- Do use a combination of numbers and letters with a mixture of upper and lower case.
- Do use a password with non-alphabetic characters, e.g., digits or punctuation.
- Do use a password that is easy to remember, so you don't have to write it down.
- Do use a password that you can type quickly without having to look at the keyboard.
- Do use a password that is at least eight characters.
- Do change your password immediately after your initial log on.
- Do change them frequently (every 2-3 months is usually adequate). This raises the security level of the passwords.
- If you forget your password and need to have it reset, call the ITS Help Desk at 740-587-6395.

### **Don'ts**

- Don't use your login name in any form (as-is, reversed, capitalized, doubled, etc.).

- Don't use your first or last name in any form.
- Don't use your spouse's or child's name.
- Don't use other information easily obtained about you. This includes your favorite food, movie, your birthday, a family member's birthday, license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
- Don't use a password with just numbers or all identical letters.
- Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.
- Don't use a password shorter than eight characters.

### **How to Choose Secure and Easy to Remember Passwords**

1. Substitute numbers and special characters for letters or words. For example: 1 = "i", 2 = to, too, two, 3 = "e", 4 or @ = "a", 5 or \$ = "s", & = and, 8 = "ate", \* = "star", @ = "at", etc.

**BE CREATIVE!**

2. Use punctuation marks, including mathematical operations, in combination with words, or between two words.
3. Choose a line or two from a song, a poem, a movie title, and use the first letter of each word.
4. Use short phrases and intentionally misspell words. Examples of good, strong passwords using many of these guidelines are shown below: (Please do not use these examples.)  
**Ez2RememBR** – This password uses the phrase "easy to remember" and a combination of upper and lower case letters and numbers to create a good, strong password.  
**c@t\$d0g5** – This password uses the words "cats" and "dogs" and a combination of numbers and special characters to create a good, strong password.

**For instructions on how to change your passwords, see:**

**[www.denison.edu/offices/computing](http://www.denison.edu/offices/computing)**

### *Additional password tools*

To see a history of your password changes or to see if the password you selected had been determined as vulnerable see:

<https://dss.denison.edu/password/history.pl>.

If the most recent date shows “VULNERABLE” then change your password immediately.

If you want a meter to check how secure possible passwords might be see:

<https://dss.denison.edu/password/meter/>

Or

<http://www.microsoft.com/protect/fraud/passwords/checker.aspx>

So, change your password, make your account more secure and remember to never give that password to anyone.

### *Notable Sayings*

Treat your password like your toothbrush – don’t share it with others and change it every few months.

Passwords are like bubble gum – strongest when fresh; should be used by an individual, not by a group; and if left lying around, will create a sticky mess!

Password Haiku:

Lowering your guard  
Sharing your secret password  
Bodes ill for you both  
- R. Chris Brown

**BE SURE TO CHECK OUT  
OUR WEBSITE FOR MORE  
INFORMATION!**

[www.denison.edu/offices/computing/](http://www.denison.edu/offices/computing/)

**Thanks to Montgomery College IT  
Security Group for the use of this  
material.**

**Information Technology Services  
Denison University  
Fellows Hall  
Granville, OH 43023  
Phone: 740-587-6395**



## **PASSWORD GUIDELINES**

### **HOW TO CREATE AND PROTECT YOUR PASSWORDS**