Open Sesame!: Desktop's Password Tips

The **DO'S** and **DON'T'S** of passwords!

- **DON'T** make the password too complicated so that you have to write it down to remember it.
- **DO** use memory tricks, if necessary, to remember your passwords.
- **DON'T** have fewer than eight (8) characters in the password because programs can easily be used to crack shorter passwords.
- **DO** be creative when creating a password.
- **DON'T** use a dictionary word so that programs can use a set list of words to guess your password.
- **DO** use a combination of upper and lower case letters, numbers, and symbols.
- **DON'T** use personal information that can be easily obtained like birthday, pet or family member's name, last name, etc.
- **DO** create **different classes** of password.
- **DON'T** ever post your password on a stick-note on your monitor.
- **DON'T** ever post your password on a stick-note under your keyboard.
- **DON'T** ever post your password on a stick-note **period**.
- **DO** be cautious when using **Password Management programs**.
- **DON'T** have your computer remember your passwords. The more you type them, the better you will remember them.
- **DON'T** email your password with the username in the same email.
- **DON'T** give your password to anyone unless **absolutely, positively, 100%, no-doubt-about-it** necessary. Even then, think carefully before you do it.
- **DO** change your password as quickly as possible, if you have any reason to believe that it has been compromised.
- **DO** be aware of Ivy Tech's **Password Policies**.
- **DO** know where to obtain the proper passwords for **Ivy Tech Classrooms**.

---

**BE CREATIVE WITH PASSWORDS**

Creative a strong password (i.e., a password not easily guessed or cracked) can be tricky. We recommend the using the following method.

1. Pick a word that:
   a. is easy to remember
   b. is more than six letters
   c. has no consecutive repeating characters, like **bookkeeper**, which has three sets of them.
d. **IS NOT** personal information like birthdays, spouse's name, etc.

e. Example 1: **doghouse**

2. Creatively misspell and mis-capitalize the word.
   1. Example 1: **dAwGhOuSe**

3. Substitute and add numbers and symbols.
   0. Example 1: **d4w&_h0uS3**
      1. Note the substitution of the numeral 4 for A, the ampersand symbol & for G, the numeral 0 for O, and the numeral 3 for e.

Example 2:

1. Step 1: **goldfish**
2. Step 2: **au ghoti** *(Au is the chemical symbol for gold; GH as in enouGH, O as it wOmen, TI as in naTIon, thus gold fish = au ghoti)*
3. Step 3: **4u&H0t1**

Example 3:

1. Step 1: **go cart** *(Note that the space counts as a character.)*
2. Step 2: **go-KarT** *(Not much you can do to mix it up.)*
3. Step 3: **g0_K@®T** *(Aha! Notice the ® symbol. You can insert symbols like this by pressing and holding the Alt key on your keyboard and typing a specific number, then lifting the Alt key. **Beware!** Novell may not be able use Alt codes. **Beware²!** If you are using a laptop, you’ll need to use its numeric keypad. Check your manual.)*

---

**REMEMBERING YOUR PASSWORD**

If you need a prompt for your password, post something in code. For example, if you had **d4w&_h0uS3** as a password, post **bowling01NIGHT**, or something else that puts you in the doghouse. Usually this type of posting is enough to jog your memory to have a successful login.

- Example 2: **dont_B_coy** *(koi)*
• Example 3: **Mahha_GoGoGo** (Transliteration of the Japanese name of the Speed Racer cartoons)

## CLASSES OF PASSWORDS

Create different classes of passwords.

- Primary passwords like banking passwords, credit card passwords and email passwords should be the most secure (strong) passwords.
- Secondary passwords would be ones like your Novell passwords — ones that change frequently.
- Tertiary passwords should be various websites that you use that contain no personal data.

You should never overlap Primary, Secondary, and Tertiary passwords. The reason why is **hackers**. A hacker will not attempt to crack your bank password due to the security imposed in those areas. But they will attempt to crack your MySpace password or other popular sites. The security on these sites is much lower than financial institutions. Once they have a password for an easy site, they may try it on your other more secure sites. If you have the same password, your account may be breached. If you have no overlap, all of the work done by the hacker was for nothing.

---

**Swordfish!: Desktop's Password Tips pt 2**

### PASSWORD MANAGEMENT

For website passwords, you may want to use a [password management](https://example.com) program like **Roboform** to keep track of the different sites. The program works usually with a **U3** ready thumb drive. **U3** is a special program that allows programs to run from a thumb drive environment.

**Roboform** runs in this type of environment to store passwords for various sites behind a master password that would be used to sign into the program. When you navigate to a site, the user will be prompted to use the stored information in the program. As long as you can remember the password to **Roboform**, you will always have access to these sites. The downside of the program is if you do not remember the password to **Roboform**, the drive gets lost, or you just forget the stored passwords, you may be locked out of the websites.
What Ivy Tech's Handbook has to say about passwords:

- "Users are responsible for maintaining the security of their assigned accounts and files. Authorized users are not allowed to share their accounts or passwords"
- "Passwords are to be changed every 30 days and not revealed to others."
- "Users may not use an account to represent anyone other than themselves, or use an account for which they do not have authority."

What it means to you:

- Do not let anyone log into your machine, SIS system, Banner system, or other College system as yourself.
- You are the only person who should have your password.
- You should not give your password to anyone even upon request. This includes supervisors and subordinates.
  - If a C&TS technician must recreate the problem in your account to fix it:
    - Never give your password to them; always sign in for them to allow them to work.
    - The people in Desktop will always ask you to sign in for them. They will never ask you for your password.
- Novell accounts are required to be changed every thirty days. Other accounts, like Banner, Campus Connect, Blackboard and email have no such restrictions at this time.
- No one else is allowed send an email as you or change grades, update information, etc. on restricted systems.

What you should do:

- If you ever have any questions about the policy or its interpretation, please feel free to talk to someone in C&TS management. At this point in time they are John Malay, Scott Kiser, and Jim Zion.
- If you think that one of these policies are being violated, please report it to a member of C&TS management.

Who manages passwords in different classroom settings

Outlying sites with our machines

- Passwords are held by site coordinators, Adjunct Advisor, Program Chairs, and Division Chairs.
It is their responsibility to verify the person who is requesting the password is who s/he says s/he is and is authorize to receive it.

People who need this information to get onto the machines may receive the password only through one of these areas.

**General Coliseum Campus/ North Campus classrooms**

- At this point in time, most of the classroom logins do not have a password associated with them.
- Accounts with special privileges on the two campus locations will have passwords associated with them. These passwords can be obtained from the **room owner**. If the passwords get out, those accounts will have their associated passwords changed immediately.

**Outlying sites without our machines**

- The **site coordinator** will have any passwords needed.

---

*Webmaster Updated 2008-10-20*