Changing a Network Password through Outlook Web Access

1. Access - Log into your e-mail account from the WCJC Internet homepage, www.wcjc.edu

2. Click on “Employee Email”.

3. Type your current information in the Domain/user name and Password boxes; Click on Log On.

You may be prompted to change your password at this point, if so see Step 8 below.

If you were not prompted to change your password, but wish to do so, see Step 4 below.

4. On the bottom left hand side, click on the Options icon.
5. Scroll down to the Password section and click on **Change Password**.

6. Enter the following:

   **Username:** wcjc\username  
   **Note:** include domain wcjc\  
   **Old Password:** Type in your current Password  
   **New Password:** Type in the New Password you want to set following the password rules.  
   **Confirm new password:** Retype, for verification, the New Password.

7. Click “OK”

8. Click the link “Back to “https://...”
9. Log in using domain and new password

Password Security Guideline

1. Purpose
   a. To provide a mechanism to maximize the security of information stored on college technology through the appropriate use of passwords.
   b. Passwords are assigned to each individual as a method to control and monitor their unique access to systems and information, and should never be shared with others.

2. Guideline
   a. Passwords expire and must be changed every 120 days.
   b. Users should change a password immediately upon suspecting it has been compromised.
   c. Users are not to give others access to systems or information by providing them with their account and password.
   d. Users are held responsible for the actions of others if they have knowingly shared their password with them.

3. Procedure
   a. Where possible, Information Technology has implemented automatic password expiration processes to ensure passwords are changed in a regular and timely manner. Otherwise, users are to change their passwords if they believe their password has been compromised. Instructions on how to change your network password are located on the WCJC Intranet at IT Training material.
   b. Microsoft Windows users are expected to abide by the following guidelines when creating or changing a password: Where possible, the password must contain at least eight characters from at least three of the following four categories:
i. English uppercase characters (A — Z)
ii. English lowercase characters (a — z)
iii. Base 10 digits (0 — 9)
iv. Non-alphanumeric (For example: !, $, #, or %)

c. **Banner INB** users are expected to abide by the following guidelines when creating or changing a password:

   i. Where possible, the password must contain at least eight characters from at least three of the following four categories:
   ii. English uppercase characters (A — Z)
   iii. English lowercase characters (a — z)
   iv. Base 10 digits (0 — 9)
   v. Non-alphanumeric to include the exclamation point (!), the period (.), or the percent sign (%)

d. **Banner Self-Service** users are expected to abide by the following guidelines when creating or changing a password:

   i. All Numeric; Six digits long

e. **WebCT** users are expected to abide by the following guidelines when creating or changing a password:

   i. Must contain at least six and not more than eight alphanumeric Characters

f. All users of information resources are responsible for assisting in the protection of the systems they use. Many intruders enter systems simply by guessing passwords and even the best passwords can eventually be defeated mathematically, given enough time. The use of strong passwords acts as a firm deterrent against password guessing attacks, and buys additional time against other attacks. All users are expected to abide by the following guidelines when creating or changing a password:

   i. Make each password unique – do not use the same password for multiple accounts or systems
   ii. **DO NOT** display your password for easy access
   iii. **DO NOT** write a password on sticky notes, desk blotters, calendars, or store it online where it can be accessed by others
   iv. **DO NOT** use a network login ID in any form (reversed, capitalized, or doubled as a password)
   v. **DO NOT** use your first, middle or last name or anyone else’s in any form
   vi. **DO NOT** use your initials or any nicknames you may have or anyone else’s
   vii. **DO NOT** use other information easily obtained about you. This includes pet names, license plate numbers, telephone numbers, identification numbers, the brand of your automobile, the name of the street you live on, and so on. Such passwords are very easily guessed by someone who knows the user
   viii. **DO NOT** use dates e.g., September, SEPT1999 or any combination thereof
   ix. **DO NOT** use keyboard sequences, e.g., qwerty_098
   x. **DO NOT** use a sample password, no matter how good, that you’ve gotten from a book that discusses information and computer security