Password Policy

The W&J user ID and password combination is required for access to most W&J network services including network log on, email, WebAdvisor, and most administrative and academic systems. The W&J password policy is intended to protect user accounts from unauthorized access. This policy applies to all W&J network account holders. Some account holders may be required to change their network password at regular intervals. Passwords are always considered private and confidential, and should be protected at all times. All account holders are responsible for protecting and maintaining their own network password, and the password for any other accounts they are assigned.

The following guidelines are required:

- A password must be at least eight characters in length, and not exceed a maximum of 20 characters. Passwords must include at least one alphabetic and one numeric character.
- W&J passwords must meet complexity requirements. To meet these complexity requirements, passwords must contain characters from three of the following five categories:
    - Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
    - Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
    - Base 10 digits (0 through 9)
    - Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/
    - Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
- Symbols and special characters such as !, @, #, $, /, and % can be used to improve the strength of the password. ***If you are a user of Ellucian Colleague, please DO NOT use special characters in your password other than !, @, #, $, /, and %. Other special characters are not compatible with Colleague and will obstruct your login to that system.***
- New passwords must be significantly different from previous passwords. You cannot use any of your previous 24 passwords.
- Never use your username, any part of your name, or any other obvious identifying characteristic like initials, birth date, telephone number, street address, social security or ID number, license plate number, name of a family member, pet, etc...
- Never write down your password or divulge it to anyone including coworkers and supervisors.

For added security, account holders may change their passwords frequently. Passwords must conform to the above standards. If you suspect your password has been compromised you should immediately change it, and then notify the ITS Helpdesk. The W&J Passport self-service portal gives account holders the ability to easily and conveniently self-manage their passwords. All account holders are encouraged to complete their PassPort profile at passport.washjeff.edu. Instructions for completing your PassPort profile can be found on the ITS wiki.

Once you have completed your PassPort profile, you will receive automatic email notifications approximately 14 days prior to the expiration date of your password. Windows PC users may also receive pop-up notifications at that time. Links to instructions for changing your password are provided below:

On-line instructions for changing your password are available. If you have any questions in regard to this process please contact the HelpDesk.