Timed Expiration and STRONG Network and System(s) Passwords

As of March, 2008, Worcester State University implemented a timed expiration policy for all user network and systems passwords. On November 17, 2008 the University implemented a 'strong' password requirement. The purposes of this to ensure the integrity these resources from unauthorized access and meet with Commonwealth and Federal mandates. What this means is that users will be asked to reset their passwords every 90 days since their most recent password change. The advantage of timed expiration along with strong passwords is to ensure that the University is in compliance with Commonwealth security regulations.

Details:

- The timed expiration policy will apply to both WSU network passwords (which are used to login to computers, access email, the community system, VPN, etc.) and Colleague. When a user's password expires, he/she will see a simple dialogue box when attempting to login to a system. This dialogue box enables the user to quickly change his/her password. Users can change their passwords at anytime by visiting the password reset application, which is available on the University's Community System's initial login page.

- In order to move into compliance with various Commonwealth regulations, as well as to better align with general IT best practices, Worcester State University has implemented a strong password requirement. The purpose of strong passwords is to better ensure the integrity of a user's login information and data by moving away from passwords that are easily guessed though common technical and social engineering means.

  There are many levels of password strength. What Worcester State University has rolled out is a protocol that requires all passwords to reflect the following elements:

  - The password must be a minimum of eight characters in length (only letters and numbers)
  - The password can not contain your username or be similar to previous 10 passwords
  - The password must contain at least one upper-case letter
  - The password must contain at least one lower-case letter
  - The password must contain at least one number

Consider your Worcester State University usernames and passwords as sensitive as your ATM PIN number or our login information for your online banking account. It is important that each member of our campus community safeguards his/her account information to help ensure the security and integrity of our systems and data. Remember, system and data security, on one level, is a shared community responsibility.

On Colleague

On February 15, 2008 the University a strong password expiration clock was applied to Colleague. On November 17, 2008 the 'strong password' requirement was applied. Authentication for Colleague is managed as part of a separate system that is segregated from the University's Windows environment, such as network login. What this means is that your Colleague username and password (if you have one) is a separate entity from your day-to-day network login. Colleague passwords can be changed in one of two ways. When a user password expires, the user will see a change password prompt when attempting to login to Colleague. This prompt is self-explanatory and enables users to easily change their passwords. The only other way to change a Colleague password is to contact the IT Help Desk, where a member of Information Technologies will reset your password for you. Please note that the WSU Network Password Lookup function (available on the Community System home page) does not apply to Colleague, nor does Windows' control-alt-delete key combination.

Additional COLLEAGUE INFORMATION:

1. When you are entering your new password, you will not see a response that the password is being entered; it will appear as though nothing is happening, but it is, in fact, taking the change.
2. The required format for your new password:

- Must contain at least 8 characters
- Must contain at least 1 upper alpha character
- Must contain at least 1 lower alpha character

  - Must contain at least 1 numeric character
  - Cannot be any variation of the login name
  - Passwords are case-sensitive

Workstation Security
It is considered good practice (and in some areas necessary to maintain HIPPA and FERPA compliance) to lock your desktop or laptop computer when it is unattended. There are two ways in which you can easily lock your desktop:

- Press control+alt+delete and select the "Lock this desktop" option or Press the Windows key+L (the Windows key is the key that's normally located between the control and alt key and is identified with a flag icon

For more information or support, visit http://uts.worcester.edu

NOTIFICATION: [various emails will continue to be sent to notify users of changes]

- If you are logged into a computer on the campus domain (WSU_domain or ACL) or virtually via VPN: click <Ctrl+Alt+Delete> and select the “Change Password” option
- If you are not connected to the campus network:
  1. visit http://community.worcester.edu
  2. BEFORE you login, you will see “WSU Network Username/Password Lookup” option locate adjacent to the Community System login fields
  3. Click the WSU Network Password Lookup link
  4. You will need your 7 Digit User ID# + Last 4 digits of your SSN# + Date of Birth to change your password. Note: the 7 digit user ID# is on your OneCard; it is not your payroll timecard number.
- When logging into Colleague at the time of your password’s expiration, a change password box will be displayed. Follow Colleague’s prompts accordingly.
- For any assistance, please contact the Help Desk at http://uts.worcester.edu or x8856.

Suggested Practices
Microsoft offers the following advice regarding password best practices:

•	Always use strong passwords. [**NOTE**: do not use special characters i.e. <, > ?#$%^&*()!@ etc.]
•	If passwords must be written down on a piece of paper, store the paper in a secure place and destroy it when it is no longer needed.
•	Never share passwords with anyone.
•	Use different passwords for all user accounts.
•	Change passwords immediately if they may have been compromised.
•	Be careful about where passwords are saved on computers. Some dialog boxes, such as those for remote access and other telephone connections, present an option to save or remember a password. Selecting this option poses a potential security threat.

Strong and Weak Passwords
Again, from Microsoft:

A weak password:

•	Is no password at all.
•	Contains your user name, real name, or company name.

•	Contains a complete dictionary word. For example, *Password* is a weak password.

A strong password:

•	Is at least seven characters long.
•	Does not contain your user name, real name, or company name.
•	Does not contain a complete dictionary word.
•	Is significantly different from previous passwords. Passwords that increment (*Password1*, *Password2*, *Password3* ...) are not strong.
•	Contains characters from each of the following four groups: upper case letters; lower case letters; numerals

You can visit Microsoft's Password Checker to evaluate the relative strength of your password:

http://www.microsoft.com/protect/yourself/password/checker.mspx