Kirkwood
COMMUNITY COLLEGE

College Procedure:	**701.1 - Password Security**
Policy Reference:	**701 – IT Security**
Responsible Department:	**Information Technologies**
Approval Authority:	**Cabinet**
Procedure Owner:	**Vice President, Information Technologies**
Effective Date:	**7/25/2013**

Version Number: 2
Legal Counsel Reviewed (yes/no): No
Legal Reference(s):
Scope: College-wide

Reason for Procedure

All network devices and accounts must be secured with appropriate user ids and passwords. Whenever possible, systems will use a unique Kirkwood Account stored in Active Directory. All Kirkwood Accounts, including those used by faculty, staff, students, contractors and partners of Kirkwood must be properly secured.

Passwords are an important part of computer security. They are the first and sometimes last line of defense. Appropriate password security is necessary to protect the College's academic interactions and daily operations.

The Procedure

Strong Passwords

Kirkwood requires strong passwords on all Kirkwood Accounts. Kirkwood defines strong passwords as having the following characteristics:

- Passwords must be at least 6 characters in length
    - For Colleague, the password length is 8
- Passwords must contain representation from 3 of the 4 character sets (Upper, Lower, Numeric, Special)
- The system will remember your previous 5 passwords, and you may not re-use them
- The minimum age of a password will be 8 days (When you change your password, you won't be able to change it again for at least 8 days)

Password Change Frequency

Kirkwood requires all passwords to be changed every six months. This reduces the likelihood of password discovery and the length of time a compromised account can be unknowingly used.

Password Storage

Choose passwords or passphrases that are easy to remember so that it is not necessary to write it on any piece of paper. A password that is written on a sticky note attached to the bottom of the keyboard, for example, does not meet protection requirements.

Password Confidentiality

Never tell another person your password. Your password should be kept completely confidential. Supervisors, coworkers, friends and family should never know your password. Likewise, it is inappropriate to ask another user for their password. If a person demands your password, refer the person to this document and contact the Office of the Executive Director of Technology Infrastructure.

Kirkwood IT administration will **NEVER**, under any circumstances, request user names and/or passwords via email. Users should treat any such requests as "phishing scams" and delete the email immediately or notify the Help Desk.

A request for password is only requested on an individual basis, when IT needs to troubleshoot an end user problem or re-image a computer. In this instance, as soon as IT has completed their tasks, the end user is encouraged to change their password.

Encryption

All Kirkwood computer systems will store passwords in an encrypted form. As such, the Help Desk cannot see or retrieve a password, only assist users in changing to a new password.

Compromised Accounts

If you suspect that a Kirkwood account has been compromised, report it to the Help Desk immediately. Compromised accounts will immediately have their password changed to prevent potential further losses.

References

Definitions

Term	Definition
Term 1	

Term 2	
Term 3	
Term 4	

Revision Log

Version Number	Date Approved	Approved by	Brief Description of Change
1	7/25/2013	Jon Neff, Vice President, Technology Services	
2		Cabinet	Procedure template 8/26/2019