ADMINISTRATIVE PROCEDURE 7.102

References Board of Trustees Policy: EP 1
Subject: Password Policy
Adopted: October 16, 2006
Review: This procedure will be reviewed by the Vice President for Finance and Administration by December 30 of each year.

Purpose

The purpose of this procedure is to:

- Reduce the risk of confidential information exposure by ensuring that passwords are kept secure, and
- Maintain high level of confidence in a password as a means to identify an individual user.

Passwords are the most important layer of protection around confidential information. Information stored electronically is at significant risk because it may be accessible from a wide variety of locations, and may be copied quickly and quietly. Passwords identify an individual employee and grant access to information. An insecure password greatly increases the risk of unauthorized access to confidential information. Because of this risk, all users of secured electronic employee systems at Elgin Community College are responsible for choosing secure passwords and keeping them safeguarded at all times.

Scope & Definitions

This policy applies to any user who electronically accesses non-public information owned or stored by Elgin Community College. A user is any administrator, faculty, staff, employee, contractor, consultant, auditor, intern, student assistant, or partner. A secured electronic employee system is any system that is non-public, contains confidential information, or where use must be restricted or monitored.

Password Complexity Requirements

These requirements apply wherever technically possible. The individual is ultimately responsible for choosing a compliant password and remaining compliant, even if the system does not enforce the requirements electronically.

- Passwords must be changed every 180 days
- A previously used password may not be re-used at a later date
- Passwords must be 8 or more characters in length
- Passwords must contain all 4 of the following character types:
    - Uppercase letters (e.g. N)
    - Lowercase letters (e.g. b)
    - Digits (e.g. 0 though 9)
    - Symbols (e.g. # ; ! < & *)

Passwords must not be based on a user's personal information or that of his or her friends, family members, or pets. (e.g. name, birthday, address, phone number, social security number)

Password Protection Requirements

- Passwords should be known to the individual owner, and no others. No user is to speak, write, or otherwise convey their password to another person, including administrators, superiors, co-workers, friends, and family members, under any circumstances.
- If a user does not have access to a system or information necessary for their job, the user must be authorized and access granted specifically to him or her.
- Helpdesk staff may need to troubleshoot problems that only occur under a specific user's ID and password. In these cases, the user should be present to type the password and monitor the use of the ID. The user is ultimately responsible for any actions taken under that ID.
- If a user either knows or suspects that his, her, or any password has been compromised, the Network Operations Department must be notified immediately, and the password must be changed immediately.
- Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, a user may input his or her password when logging on to an officially supplied off-campus service such as AccessECC, ENet, Cisco VPN, and Citrix.
- No user is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, it must be kept in a locked file cabinet, or encrypted file if in electronic form.
- Do not use the "Remember Password" feature of applications.
- A user's passwords on College systems should not be identical or similar to passwords used on non-college systems such as online services, web forums, online banking, or newsletter subscriptions.
- The Network Operations Department may attempt to *crack* or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

Enforcement

Violation of this policy is subject to appropriate disciplinary action including termination of employment.