PASSWORD MANAGEMENT PROCEDURE

Related Board of Trustees Policy: BP 8.4
Approval: August 2012
Revision:
NC Statewide Technology Standard(s): 20106

Purpose: To prevent unauthorized access and to establish user accountability when using IDs and passwords to access College information systems.

All users must be properly identified and authenticated before being allowed to access Craven information systems. The combination of a unique User ID and a valid password shall be the minimum requirement for granting access to an information system when IDs and passwords are selected as the method of performing identification and authentication. A unique user ID shall be assigned to each user so that individual accountability can be established for all system activities. Management approval shall be required for each user ID created.

Password management capabilities and procedures shall be established to ensure secrecy of passwords and prevent exploitation of easily guessed passwords or weaknesses arising from long-life passwords. When IDs and passwords are selected as the method of performing identification and authentication, the College is required to select and use the appropriate standards and best practices.

- For secured access to systems and applications that require a low level of security, passwords shall have at least six (6) characters of any sort.
- For access to all systems and applications that require a high level of security, such as electronic fund transfers, taxes and credit card transactions, passwords shall be at least eight (8) characters.
- To the extent possible, passwords shall be composed of a variety of letters, numbers and symbols with no spaces in between.
- To the extent possible, passwords shall be random characters from the required categories of letters, numbers and symbols.
- Passwords shall not contain dictionary words or abbreviations.
- Password generators that create random passwords shall be allowed.

Password Management Standards

Passwords shall not be revealed to anyone, including supervisors, family members or co-workers. In special cases where a user must divulge a password, such as for system support, the user shall immediately change the password after the purpose for revealing the password has been achieved.

- Users shall enter passwords manually, except for simplified/single sign-on systems that have been approved by the College.
- Passwords shall not be stored in clear text on hard drives, diskettes, or other electronic media. If stored, passwords shall be stored in encrypted format.
- Password Changes:
  - Employees and contractor passwords (e.g., e-mail, web and calendar) used to access systems and applications shall be changed at least every ninety (90) days. Passwords shall be different by at least 3 characters from the previous password.
- Passwords shall not be inserted into e-mail messages or other forms of electronic communication without proper encryption. Conveying a password in a telephone call is allowed when a positive identification has been established. Conveying a password in person shall require appropriate identification if the user is not known.
- Where possible and practical, access to password-protected systems shall be timed out after an inactivity period of thirty (30) minutes or less or as required by law.
- Passwords shall be changed whenever there is a chance that the password or the system could be compromised.

Return to the Table of Contents