3357:13-19-421 Information Technology System Password Standards

(A) The password policy (19-42) is an important part of the College's overall protection of information, protection against unauthorized modification of information, protection of systems against denial of service attacks, and protection of systems against unauthorized access. As such, it applies to all accounts used to access North Central State College resources including all hosted systems. This policy and accompanying requirements covers all system users at any location, including those faculty, students and staff using privately owned computers or systems to access College information, and network resources.

(B) The purpose of these associated standards are to emphasize the importance for the creation of strong passwords, the protection of those passwords, and the frequency of password changes.

(C) Passwords Standards:

(1) Passwords will not contain the user's account name or parts of the user's full name that exceed two consecutive characters.

(2) All passwords must be at least eight characters in length and contain characters from three of the following four categories:

(a) English uppercase characters (A through Z)

(b) English lowercase characters (a through z)

(c) Base 10 digits (0 through 9)

(d) Non-alphabetic characters (for example, !, $, #, %)

(3) Failed Login Attempts: After 5 failed attempts to enter a password the account will be locked out for 15 minutes.

(4) Complexity requirements: Password standard and complexity requirements are enforced when passwords are changed or created.

(5) Enforce password history: Users must go through 12 passwords before they can reuse a previous password.

(6) Maximum password age: After 90 days the system will require the user to change their password.

(D) User Obligations

(1) Obligations on NCSC System End Users for Maintaining Security of NCSC Passwords

Do not share North Central State College passwords with anyone, including other NCSC employees, part time or temporary employees, College work-study students, and student workers. All passwords are to be treated as sensitive information.

(2) Obligations on NCSC System End Users for Notification of Suspected Compromised Password

(a) If an account or password is suspected to have been compromised, report the incident to the Information Technology Services Service Desk and change all passwords.

(b) Application developers must ensure their programs contain the following security precautions:

(i) Must support authentication of individual users not groups

(ii) Must not store passwords in clear text or in any easily reversible form.

(E) Unattended Computers

(1) To protect against unauthorized access to data on computers left unattended the following precautions are required:

(a) Enable password protection on the screen saver for all College computers with the exception of special purpose computers designed for public access such as registration kiosk computers. The length of time before the password-protected screen saver comes on should be set to 20 minutes or less.

(b) Never leave your computer unattended and unprotected. Before leaving your office computer, lock the display or log out in a manner that requires a password to gain access.

(c) Idle Account Lock: If a PC is idle for 20 minutes it will automatically lock requiring a password to continue.

(F) Single Sign-On Through Password Synchronization (For System Admins)

Since most systems and applications make at least some effort to protect their passwords, synchronized passwords are normally more secure. To mitigate the risk of a single system compromise being leveraged by an intruder into a network-wide attack, there are some password management guidelines to follow:

(1) Responsibility of System Admins

(a) Synchronize passwords across all systems

(b) Provide single sign-on authentication across all application systems (e-mail, computer, Ellucian administration systems, etc.)

(c) Synchronized passwords will be changed regularly, on the assumption that either some in-scope systems are vulnerable or that passwords may be compromised through non-digital means (social engineering, etc.).

(2) Responsibility of System Users

Users will be required to select strong (hard to guess) passwords when synchronization is introduced.

(G) Violations of the Password Policy (19-42) and/or Information Technology Password Standards (19-421) may be subject to disciplinary action, up to and including termination of employment depending on the complexity or severity of the violation.

(H) References

- http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf
- http://hitachi-id.com/password-manager/docs/password-management-best-practices.html
- http://militarycac.com/files/army_password_standards.pdf
- http://technet.microsoft.com/en-us/magazine/ff741764.aspx

Effective: November 1, 2014
Expires: November 1, 2019
Review Dates: 11/1/2014