Password Policy

(Issued on February 9, 2004 by Chancellor Herzog)

I. INTRODUCTION

This Policy governs password creation, usage and protection within the Connecticut Community Colleges (CCC).

User authentication is the means by which an Information Technology (IT) Resource authorizes a user by verifying that the user provided the correct identity. The following factors can be used to authenticate a user. Any of these by themselves or in any combination can be used:

- Something you know – password, Personal Identification Number (PIN)
- Something you have – Smartcard
- Something you are – fingerprint, voice scan etc.

Passwords are the most widely used user authentication factor. They are an important aspect of computer security by providing the front line of protection for user accounts. A weak password may result in the compromise of CCC's entire network. As such, all authorized users of CCC IT Resources are required to take appropriate steps, as outlined below, to select and secure their passwords.

II. GENERAL PROVISIONS

A. PURPOSE

The purpose of this Policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

B. SCOPE

This Policy applies to:

- All individual users (CCC students, faculty, staff, and others affiliated with CCC, including but not limited to those in program or contract relationship with CCC), who use the IT resources provided by CCC.
- All IT resources owned or managed by Connecticut Community Colleges (CCC).

C. DEFINITIONS

The following terms are used in this Policy. Knowledge of these definitions is important to an understanding of this Policy:

IT Resources: This includes, but is not limited to, computers, computing staff, hardware, software, networks, computing laboratories, databases, files, information, software licenses, computing-related contracts, network bandwidth, user IDs, passwords, documentation, disks, CD-ROMs, DVDs, magnetic tapes, and electronic communication.

Password: A string of characters which serves as authentication of a individual's identity, which may be used to grant, or deny, access to private or shared data.

Password History File: An encrypted file that contains previous passwords used by the User ID.

Password Lifetime: The length of time a password may be used before it must be changed.

Strong Password: Strong passwords are constructed of a sequence of upper and lowercase letters, numbers, and special characters, depending on the capabilities of the operating system or application. Typically, the longer the password the stronger it is. Passwords must be unique across all IT resources and not easily tied back to the user such as: User ID, given name, social security number, telephone, employee number, phone or office numbers, address, nicknames, family or pet names, birth date, license plate number, etc.

User Account: The user account is made up of the User ID and password.

User: The individual requesting a user account in order to perform work in support of a CCC program or a project, by accessing the CCC computer network.

User ID: Also referred to as a username. A User ID identifies the user on the system and has an associated password.

D. RESPONSIBILITIES

Policy. This Policy was issued by the Chancellor of the CCC after consultation with appropriate councils, including the Council of Presidents and the Information Technology Policy Committee.

Implementation. In support of this Policy, system standards and procedures shall be developed, published and maintained. And where CCC standards and procedures do not exist, each college is responsible for policy implementation.

Informational Material. Each college shall ensure that users of the CCC IT resources are aware of all IT policies, standards and procedures as appropriate.

E. VIOLATION OF POLICY

The CCC considers any violation of this Policy to be a serious offense and reserves the right to copy and examine any files or information resident on CCC IT resources to ensure compliance. Violations of this policy should be reported to the appropriate CCC authority.

Disciplinary Actions. Violators of this Policy may be subject to disciplinary action up to and including dismissal or expulsion pursuant to applicable Board policies and collective bargaining agreements.

III PASSWORD CRITERIA

When composing a password, it must adhere to the following standards:

- Passwords must be a minimum of eight (8) characters.
- Passwords must be complex and difficult to guess. (strong passwords must be used)
- Password must not be reused. (verified against a password history file that is set to the maximum size that the system supports)
- Password must be changed every ninety (90) days. (maximum lifetime)

When using a user account, the following standards must be enforced:

- User accounts must be locked out for a period of time after a maximum of five (5) unsuccessful attempts to gain access to a user account.
- If any part of the logon process (User ID, Password, etc.) is incorrect, the user must not be given specific feedback indicating the source of the problem. Instead, the user must simply be informed that the entire logon process was incorrect.
- Passwords issued by a password administrator must be pre-expired, forcing the user to choose another password before the logon process is completed.

IV PASSWORD PROTECTION

All passwords shall be treated as sensitive, confidential CCC information and therefore must be protected as such:

- All vendor-supplied default passwords for software, application and devices must be changed before any IT resource is used on the CCC's network.
- Passwords must not be reset by a password administrator without the user first providing definitive evidence substantiating his or her identity.
- Passwords issued by a password administrator must be unique and must be sent via a communications channel other than the channel used to log-in to the system.
- Passwords must never be shared or revealed to anyone other than the authorized person. Passwords must not be written down on any medium.
- Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, devices without access control, dial-up communications programs, Internet browsers, cookie files or in other locations where unauthorized individuals might discover or use them.
- Users must refuse all offers to place a cookie on their computer so that they can automatically log on the next time they visit the site.
- Passwords must immediately be changed if the user suspects their user ID or password has been disclosed to an unauthorized person or if a system has been compromised or is under the suspicion of having been compromised.

V. DISCLAIMER

CCC disclaims any responsibility for and does not warranty information and materials residing on non-CCC systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of CCC, its faculty, staff or students.

VI. NOTICE TO USERS

As laws, technology and standards change from time to time, this Policy may be revised as necessary to reflect such changes. It is the responsibility of users to ensure that they have reference to the most current version of CCC Policies.