Collin College Technology Services (CC-TS)
User Accounts Password – Information Security Procedure (ISP)

PURPOSE:

All user accounts will be protected by passwords that are both strong and confidential. Users will protect the security of those passwords by managing passwords according to CC-TS password ISP.

System and Application Administrators will ensure account passwords are secured using industry best practices.

SCOPE:

The Collin College (CC) User Accounts Password ISP applies equally to all individuals granted access privileges to any Collin College information technology resources.

STATEMENT:

Users are responsible for what is accessed, downloaded, or created under their credentials regardless of intent. An unauthorized person can cause loss of information confidentiality, integrity, and availability, resulting in liability, loss of trust, or embarrassment to CC.

Account holder’s responsibilities:

1. Must create a strong password and protect it.
2. Password must have a minimum length of eight (8) alphanumeric characters.
3. Password must contain one upper case, one lower case, and one numeric character.
4. Passwords must not be easy to guess. For instance, they should not include part of your social security number, birth date, nickname, etc.
5. Passwords must not be easily accessible to others (e.g., posted on monitors, under keyboards).
6. Computing devices must not be left unattended without locking or logging off of the device.
7. Stored passwords must be encrypted.
8. CC username and password should not be used for external services (e.g., LinkedIn, Facebook, or Twitter).
9. Users should never share their passwords with anyone, including family, supervisors, co-workers, and CC-TS personnel.

10. Users will be required to change passwords at least once annually.
11. If you know or suspect that your account has been compromised, change your password immediately and contact CC-TS Help Desk for further guidance and assistance.
12. If CC-TS suspects your account has been compromised, your account will be deactivated, and you will be contacted immediately.

Any individuals responsible for managing passwords must:

1. Prevent or take steps to reduce the exposure of any clear text, unencrypted account passwords that CC applications, systems, or other services have received for authentication purposes.
2. Never request that passwords be transmitted unencrypted. Passwords must never be sent via email.
3. Never circumvent this password ISP for the sake of ease of use.
4. Coordinate with CC-TS regarding password procedures.

Detailed information and instructions for password management can be found on the CC website.

https://www.collin.edu/academics/ecollin/onelogin/OneLoginPassword.pdf

DEFINITIONS:

Compromised Account: The unauthorized use of a computer account by someone other than the account owner.

Encrypted: The conversion of data into a form called cipher text that unauthorized people cannot easily understand. Encryption is achieved using Windows native Bit Locker or other available software.

Password: A string of characters input by a system user to substantiate their identity, authority, and access rights to the computer system that they wish to use.

System Administrator: Individual(s) who are responsible for running/operating systems on a day-to-day basis.

Unauthorized person: Any person who has not been given official permission or approval to access CC systems.

Related Policies, References, and Attachments:

An index of approved CC-TS policies can be found on the CC Information Technology Services Policies website at https://www.collin.edu/security.