Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
User Accounts Password Policy:

PURPOSE:

Strong and confidential passwords will protect all user accounts. Users will protect the security of those passwords by managing passwords according to Clarendon College-IT password procedures.

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

SCOPE:

The Clarendon College User Accounts Password policy applies equally to all individuals granted access privileges to any Clarendon College information technology resources.

POLICY:

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

Account holder's responsibilities:

1. Must create a strong password and protect it.
2. The password must have a minimum length of eight (14) alphanumeric characters.
3. Password must contain a mix of upper case, lower case, and numeric characters and special characters (!@#%^&*+=?/~';:,<>|\).
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 or 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. Clarendon College username and password should not be used for external services (e.g., LinkedIn, Facebook, or Twitter).
9. Users should never share passwords with anyone, including family, supervisors, co-workers, and Clarendon College IT personnel.

10. Users must change passwords at least once every 365 days, reference NIST SP-800-63 (NIST Password Guidelines | AuditBoard).
11. If you know or suspect your account has been compromised, change your password immediately and contact Clarendon College-IT for further guidance and assistance.
12. If Clarendon College-IT suspects your account has been compromised, your account will be deactivated, and you will be contacted immediately.
13. Employees must use Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA) with their network and PC access passwords. Student use of 2FA/MFA is also encouraged.
14. Recording login information on paper notes or other unsecured means is prohibited. Using electronic password managers to store and record user login credentials is highly encouraged and is available.

Any individuals responsible for managing passwords must:

1. Prevent or take steps to reduce the exposure of any clear text or unencrypted account passwords that Clarendon College applications, systems, or other services have received for authentication purposes.
2. Never request that passwords be transmitted unencrypted. Passwords must never be sent via unsecured email. If email is used to transmit login information, it must be sent via a secure email process.
3. Never circumvent this password policy for ease of use.
4. Coordinate with Clarendon College-IT regarding password procedures.

DEFINITIONS:

Clarendon College IT: Individuals or contractors that work or perform duties on behalf of the Clarendon College IT Department.

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 they wish to use.

System Administrator: Individual(s) responsible for running/operating systems daily.

Multi-Factor Authentication (MFA): this security measure requires more than one form of identification to log into an account. It's also known as two-step verification.

Two-Factor Authentication (2FA): an identity and access management security method that requires two forms of identification to access resources and data. 2FA allows businesses to monitor and help safeguard their most vulnerable information and networks.

Secure Email Services: Secure email services use encryption and identity checks to protect your messages. Some of the most secure email providers include Mimecast, Barracuda, and Proton.

Unauthorized person: A person without official permission or approval to access Clarendon College systems.

Password Manager: is a software program that stores and manages passwords for online accounts. It can also generate strong passwords and automatically fill in forms, i.e., Keeper.

Related Policies, References and Attachments:
An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at https://www.clarendoncollege.edu/information-technology. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on March 27, 2025, version 1.3. This policy was reviewed by Will Thompson, Vice President of IT, on February 13, 2025.