Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
User Account Credentials Management Policy:

PURPOSE:
The purpose of this policy is to establish standards for the administration of user account credentials that access Clarendon College information technology resources. These resources must be protected from unauthorized access, loss, corruption, or destruction, thus ensuring the confidentiality, integrity and availability of these resources. Proper management of account credentials provides a means of assuring accountability and protecting Clarendon College resources. The standards established in this policy include issuing account credentials, granting access to approved resources, account credential maintenance and deactivation processes.

Scope:
The Clarendon College User Account Credentials Management policy applies to those responsible for the management of user account credentials on Clarendon College information technology resources.

Policy Statement:
Creating unique domain user account credentials is an automated process utilizing the current approved Clarendon College account naming convention and is based on assigned roles within the ERP system (e.g. faculty, staff, student worker, student, visitor, alumni, etc.) The level of authorized access will be based on the principle of least privilege (PoLP), but if a user is assigned multiple roles, the most privileged role will take precedence.

1. The creation of a user account credential issues a unique, non-transferable electronic identity known as the "username" and a corresponding "password". Usernames will remain in effect throughout the individual's official affiliation with Clarendon College. (User Account Credentials Eligibility).
2. Usernames are not reused.
3. When an individual changes roles or ends their affiliation, Clarendon College-IT deactivates the user account credentials that no longer meet Clarendon College's eligibility requirements (User Account Credentials Eligibility) and removes non-standard access.
4. Upon user activation, account holders are authorized to access the resources dictated by their role membership.
5. Clarendon College-IT requires users to change passwords per User Account Credential Password Policy.
6. Requests for exceptions to this policy must be submitted in writing (Clarendon College-IT Policy Exception Form) to the Information Security Officer (ISO) or Vice President of Information Technology and will be reviewed on a case by case basis. Requests shall be justified, documented, and communicated as part of the risk assessment process.

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. Reference materials, legal compliance guidelines, and policy enforcement are available in the Policy Compliance Document. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

This policy was approved by the Clarendon College Board of Regents on July 17, 2023, version1.1. This policy was reviewed by Will Thompson, Vice President of IT on July 15, 2023.