Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Identification/Authentication Policy:

PURPOSE:
The purpose of the Identification/Authentication Policy is to ensure the security and integrity of Clarendon College data and information technology resources by ensuring controls for securing user identification and authentication credentials.

To ensure the security and integrity of Clarendon College data, identified users will securely authenticate to Clarendon College information technology resources and access only resources which they have been authorized to access.

If user identities are not properly authenticated, Clarendon College has no assurance that access to information technology resources is properly controlled. This policy will mitigate the risk of unauthorized access of information, as well as establish user accountability and rules for access.

SCOPE:
The Identification/Authentication Policy applies to all individuals granted access to Clarendon College information technology resources.

POLICY STATEMENT:
Clarendon College shall require that systems are protected from unauthorized access by establishing requirements for the authorization and management of user accounts, providing user authentication (any or all of the basic authentication methods), and implementing access controls on Clarendon College information technology resources. Access control is provided at the firewall, network, operating system, and application levels.

Clarendon College managers/supervisors have the responsibility of requesting access to information systems and approving user access privileges based upon their assigned duties, as well as notifying Data Owners and Clarendon College-IT of the termination of access to information technology resources.

Prior to being granted access to Clarendon College information technology resources, the needs of the employee, student worker, contractor, vendor, guest, or volunteer shall be given ample consideration and authorization granted to allow access to Clarendon College information technology resources. Access should be granted according to the principle of least privilege as outlined in IT Administrator/Special Access Policy.

Clarendon College accounts will have a unique identifier that is associated with a single user. Once an identifier is assigned to a particular person, it is always associated with that person. It is never subsequently reassigned to identify another person.

Use of the authentication service to identify oneself to a Clarendon College system constitutes an official identification of the user to the College, in the same way that presenting an ID card does. Security is everyone's responsibility, and everyone has a responsibility to protect their own "identity". Users will be held accountable for all actions of their accounts.

Regardless of the authentication method used, users must use only the authentication information that they have been authorized to use; i.e., must never identify themselves falsely as another person. Additionally, users must keep their authentication information confidential; i.e., must not knowingly or negligently make it available for use by an unauthorized person. Anyone suspecting that their authentication information has been compromised should contact the Information Security Officer immediately.

Users must adhere to the requirements of the Clarendon College User Accounts Password Policy.

Clarendon College Data Owners shall be responsible for ensuring that authorization and account management processes are documented and that the appropriate people have been assigned the responsibility of creating and maintaining authorization records.

Clarendon College Data Owners may monitor related activities of individuals as a condition for continued access. At a minimum, Clarendon College Data Owners must review user access privileges annually.

DEFINITIONS:

Authentication Credentials: The verification of the identity of a user who wishes to access a system, commonly using a password in conjunction with a unique UserID.

Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department that has the responsibility for maintenance and supervision of the Clarendon College IT infrastructure.

Data Owner: Departmental position responsible for classifying business data, approving access to data, and protecting data by ensuring controls are in place.

Mitigate: The elimination or reduction of the frequency, magnitude, or severity of exposure to risks in order to minimize the potential impact of a threat.

Principle of Least Privilege: The practice of limiting user profile privileges on computers to only the information and resources that are necessary, based on users' job necessities.

Unauthorized Access: Access by a person who has not been given official permission or approval to access Clarendon College systems.

User Identification: A unique sequence of characters used to identify a user and allow access to a computer system or computer network.

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.