Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Third Party Access Policy:

PURPOSE:
Clarendon College receives requests for direct connections to its information technology resources from contractors, vendors and other third parties for support services, contract work or other remote access solutions for the College.

The purpose of this policy is to define standards for connecting to Clarendon College information technology resources. These standards are designed to minimize the potential exposure to Clarendon College from damages which may result from unauthorized use of Clarendon College information technology resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical Clarendon College internal systems, etc.

SCOPE:
The Third Party Access Policy pertains to all third party organizations and individuals that require access to non-public electronic resources maintained by Clarendon College.

POLICY STATEMENT:
As a condition of gaining access to Clarendon College information technology resources:

1. Every third-party must sign a Clarendon College Non-Disclosure Agreement.
2. All third parties must be sponsored by a Clarendon College department, organization or employee.
3. All third-party access must be uniquely identifiable and password management must comply with the User Accounts Password Policy (IC) and IT Administrator/Special Access Policy (IS) guidelines.
4. All third-party account holders must provide contact information that will be used to contact them in the event of account status changes, misuse, or termination of the agreement.
5. All changes to access granted under this policy must originate from the Clarendon College sponsor and are subject to a security review.
6. Third parties must be made aware and must comply with all applicable Clarendon College policies, practice standards, agreements and guidelines, including but not limited to:
    a) Acceptable Use Policy
    b) Encryption Policy
    c) Privacy Policy
    d) Network Access Policy
    e) Portable Computing Policy
    f) Change Management Policy
    g) Clarendon College Information Security Program
7. Third-party agreements and contracts must specify:
    a) The Clarendon College information to which the third party has access.
    b) How Clarendon College information is to be protected by the third party.

c) Acceptable methods for the return, destruction or disposal of Clarendon College information in the third party's possession at the end of the contract.

8. Third parties must only use Clarendon College information and information technology resources for the purpose of the business agreement.
9. Any other Clarendon College information acquired by the third party in the course of the contract cannot be used for the third party's own purposes or divulged to others.
10. Third-party personnel must report all security incidents immediately to the appropriate Clarendon College sponsor and the Information Security Officer (ISO).

Any third-party account holder that violates this policy will have the account suspended and the account holder's sponsor will be notified. Following a review, Clarendon College will implement the actions specified by the ISO to reinstate or remove the account.

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.