Whenever Cedar Crest College purchases a product, there may be a situation when a vendor or support technician will need to get in to the Cedar Crest College network or on to a Cedar Crest College computer/server. The purpose of this document is to detail the methods that non-Cedar Crest individuals are authorized to use in order to provide support to the systems on campus.

This policy is designed to allow access from the outside of the Cedar Crest network to devices inside the network in as easy a manner as possible while minimizing security risk, reducing the potential for unauthorized access to Cedar Crest resources, minimizing the risk of systemic damage and reducing any chance of an outside vendor making alterations or changes without the authorization of Cedar Crest College staff. Damages include the exposure of sensitive or confidential information, damage to the performance of production systems or any incident which may damage the public image of the college.

This policy applies to all Cedar Crest College employees, contractors or vendors doing work on behalf of Cedar Crest College. This policy applies to work on college owned computers, servers, network equipment, video equipment or any other device that is connected to the Cedar Crest College network.

Access Credentials

- All vendors needing to set up any long term support connections must furnish the Office of Information Technology with a formal document that states what system the support is for, and how and when support will be provided. Access credentials to internal systems will only be active when a support issue is active. All credentials/access will be deactivated during times when systems are functioning normally.
- All access to college owned systems or any system that houses college owned data will be facilitated via a named, Active Directory-based account that is setup and managed by the Office of Information Technology.
- In the event that a system requiring support is not joined to the Active Directory domain, other credentials will be set up and provided by the Office of Information Technology in conjunction with the vendor.
- No generically named access accounts to systems will be allowed.
- Under no circumstances will a vendor be allowed access to any internal system without the prior knowledge and authorization of a Cedar Crest College employee and the Office of Information Technology.

Network Access

- The primary method for access to a system on the network will be via a names, vendor specific account through the Palo Alto GlobalProtect VPN Client. This client exists for both Windows and Macintosh computers, and should be accessible by any vendor. This will then allow for the vendor to connect to the device via HTTP, HTTPS, RDP, Telnet or SSH based on security settings. If another protocol is necessary, the request can be made through the Office of Information Technology.
- In the event that the vendor/contractor cannot download and install the VPN client for one reason or another, they may connect to the system via a TeamViewer connection.
- Any and all specific information related to remotely accessing the Cedar Crest College network will be provided to vendors on a case by case basis by the Office of Information Technology.

The Office of Information Technology reserves to right to disable, remove or refuse access to the Cedar Crest network in the event that this policy has been violated or the security of the network or its resources is compromised.

The latest version of this document can be found on the Cedar Crest College website at: http://help.cedarcrest.edu