

VII:01:21 REMOTE ACCESS TO COMPUTER RESOURCES

The computer resources are available to all students, faculty and staff upon written application and authorization by the Director of Information Technology. It is the responsibility of Information Technology personnel to maintain a stable operational environment for all users and to provide security for all programs and data residing on available computer systems. Cooperation of all users in the form of ethical and responsible behavior is required at all times so that all can share resources freely and equitably.

The computer resources of the College are available through non-local (Remote) access on a limited basis. Due to the nature of this type of access, additional controls are required. Individuals requesting access to the system through remote network connections agree to the following conditions:

1. Under no circumstance will a user authorized for remote access grant the use of and/or access to their account to any other party.
2. Under no circumstance will a user authorized for remote access disclose College node names or IP addresses to any other party.
3. Under no circumstance will a user authorized for remote access store or record a username, password, node name, or IP address on any electronic device.
4. Users authorized for remote access understand that their connection may be terminated at anytime, possibly without warning due to a higher priority request for a shared resource. Usually effort will be made to notify the user prior to process termination.
5. Users understand that this policy in no way supersedes those policies set forth in the policy on Use of Computing Resources (VII:01:01) or any other College policy.
6. Users understand that approval for remote access to the College's information resources in no way implies an obligation of the College to provide, install, or test any hardware or software at the user's remote location.

Users requesting remote access must formally request such access from and provide written justification for such access to the Director of Information Technology.

The dispositions listed below (not an all-inclusive list) for violations to this policy are examples drawn from the sanctioned policy of the Tennessee Board of Regents' Policy on Student Conduct and Disciplinary Sanctions.

1. Revoking of the individual's right to use the computer, either on a temporary or permanent basis.

2. Probation.
3. Suspension.
4. Expulsion.
5. Financial assessment for computer services.
6. Legal prosecution.

In the event that other College regulations are violated, additional penalties may be imposed.

Unauthorized use of any College computer system by an individual may be adjudged a felony, and the individual may be liable to legal prosecution.

VSCC Source: September 1, 1993, President; February 29, 2008, President