PROCEDURE:
3.3.4p4. Remote Access

Revised: *February 16, 2011; February 20, 2013; February 18, 2015; February 17, 2016; February 15, 2017; February 21, 2018*
Last Reviewed: *February 16, 2011; February 15, 2012; February 20, 2013; November 20, 2013; February 18, 2015; February 17, 2016; February 15, 2017; February 21, 2018; November 28, 2018; February 19, 2020; February 17, 2021; February 16, 2022; January 18, 2023*
Adopted: *August 20, 2008*

I. PURPOSE

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

II. RELATED AUTHORITY

TCSG Procedure 3.3.4p. Acceptable Computer and Internet Use
Ogeechee Technical College Procedure 3.3.4p2. Email Use
Ogeechee Technical College Procedure 3.3.4p3. Privacy Notice to Computer Users

III. APPLICABILITY

This procedure applies to all remote access connections for College employees, contractors, vendors, and agents who connect to the College's network.

IV. DEFINITIONS

VPN: Virtual Private Network is a method for accessing a remote, secure network via the public Internet.

Dual Homing/Split-Tunneling: The practice of establishing connectivity to more than one network at a time from a single device. For example, while connected to the College VPN, no other network connections should be established until the VPN is disconnected.

V. ATTACHMENTS

None.

VI. PROCEDURE

General

1. It is the responsibility of College employees, contractors, vendors and agents with remote access privileges to the College's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the College.

2. Use of the College’s network resources via remote access is limited to the authorized user only.
3. Only College provided remote access methods are permitted to remotely access college resources.
4. No outgoing remote connection method is allowed at any time without the express consent of the Information Security Officer.

Requirements

1. At no time should any College employee, contractor, vendor or agent with remote access privileges provide their login or email password to anyone.
2. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
3. Non-standard hardware configurations must be approved by the Information Technology Services Department.
4. All devices that are connected to the College's internal networks via remote access technologies must use up-to-date operating systems and anti-virus software.

Enforcement

Abuse or misuse of computing/information technology services may violate this procedure, but it may also violate criminal statutes. Therefore, the College will take appropriate action in response to user abuse or misuse of computing/information technology services. Action may include, but not necessarily limited to, the following:

1. Suspension or revocation of computing privileges;
2. Reimbursement to Ogeechee Technical College for resources consumed;
3. Other legal action including action to recover damages;
4. Referral to law enforcement authorities;
5. Computer users (faculty, staff and/or students) will be referred to the appropriate office for disciplinary action, which could result in suspension/expulsion of a student or suspension or dismissal of an employee.

VII. RECORD RETENTION

Documents associated with the abuse or misuse of computing/information technology services and any associated disciplinary action should be maintained for a period of two (2) years after the completion of litigation.