Remote Network Access Policy

Area: Information Technology Services	Number:	
Subject: Remote Access Management	Issued:	8/6/2012
Applies To: University	Revised:	
Sources:	Updated:	
	Reviewed:	
Responsible Party: Vice President for Information Technology	Page(s):	Page **1** of **2**

I. Purpose

Access to University IT resources from off-campus locations has increased due to the proliferation of teaching, research, and administrative applications and the increased mobility of faculty and staff. Opening unsecured and uncontrolled paths to University IT resources presents significant risks to the University community and IT infrastructure. Appropriate controls and protections are required in order to mitigate these risks, preserve and protect University IT assets.

II. Policy Statement

Rationale

Access to University IT resources from off-campus locations has increased due to the proliferation of teaching, research, and administrative applications and the increased mobility of faculty and staff. Opening unsecured and uncontrolled paths to University IT resources presents significant risks to the University community and IT infrastructure. Appropriate controls and protections are required in order to mitigate these risks, preserve and protect University IT assets.

Scope

This policy applies to all Georgia Southern authorized employees, contractors, vendors and authorized persons using any device connecting to the Georgia Southern network and/or through any other network service.

Definition

Authorized persons connecting to non-public IT resources through facilities other than the University's network shall be determined to be Remote Access.

Policy

1. Remote Access is subject to the University's Appropriate Use Policy and extends to authorized persons who may not be students or employees of the University;

2. The Chief Information Officer (CIO) will designate management responsibilities of Remote Access.
    a. For the purposes of this policy the Director of Network and Telecom and the Chief Information Security Officer are so designated.

3. The CIO or his/her designee(s) will authorize users, define methods, establish procedures and operate systems for Remote Access and document these elements as a Remote Access Standard.

Enforcement

The CIO is responsible for enforcement of this policy. Violations of this policy can lead to disciplinary action up to and including dismissal, and/or legal action. Any known violation of this policy is to be reported to the CIO or his/her designee.

Related Documents

Virtual Private Network (VPN) Policy
Acceptable Use Policy
Remote Access Standard