Remote Access Standards

Area: Information Technology Services	Number:	
Subject: Remote Access Management	Issued:	8/1/2012
Applies To: University	Revised:	
Sources:	Updated:	
	Reviewed:	
Responsible Party: Vice President for Information Technology	Page(s):	Page **1** of **3**

I. Purpose

University System of Georgia Board of Regents Policy Section 11.1 established that the Board of Regents shall rely on the Chancellor, the presidents of all USG institutions, and their chief information officers to develop, adapt, and administer the information technology methods and procedures for promoting efficiency of operations and the advancement of learning. Hence, University is tasked with the responsibility of controlling access to student, employee and other high risk, restricted and/or confidential records under FERPA (Family Educational Rights and Privacy Act), GLB (Gramm-Leach-Bliley) and other legislation. To that end, the University requires that remote access to high-risk, restricted and/or confidential records be encrypted during travel over public or unsecured networks (e.g. the Internet).

II. Policy Statement

1. **Remote access to the Georgia Southern University network and systems:**
    a. Any person remotely accessing any University network resources must adhere to all University policies and standards to ensure University resources are adequately protected.
    b. Administrative duties that need to be performed on any university system technology resource (router, switches, servers, computers, etc.) must use the university's centrally managed VPN that provides encryption and secure authentication.
    c. Any unencrypted remote access applications must not be used, such as telnet and VNC.
    d. Remote access tools used from off-campus to access systems on campus may only be used when in conjunction with the university VPN.
    e. Only authorized remote control services may be used. (See section 4a.)
    f. Individuals who remotely access University data must manage said university data as defined in the Data Stewardship and Classification Standards document.
    g. The Director of Network and Telecom will be contacted for approval when the use of a VPN is not viable, when additional controls are required, or for exception requests.

h. Remote access may be blocked at any time for any reason determined by the Chief Information Security Officer or the Director of Networking and Telecom, but generally considering the following:
    i. Failure to adequately protect University data.
    ii. Evidence of security compromise in login credentials and/or hardware or software used for access.
    iii. Any violation of the Georgia Southern Acceptable Use Policy.
    iv. Blocked access may be reinstated with verification that the problem(s) that resulted in access being blocked have been adequately addressed and resolved.

2. **Access/Authentication**
    a. The access and authentication system for remote access will be centrally managed by IT Services.
    b. User accounts and passwords are used to establish individual accountability within the university's VPN. Concurrent with the Appropriate User Policy, users are not to divulge their passwords for any reason. For example, user accounts are not to be shared, and any activity performed by a particular user account will be the full responsibility of the person assigned to that user account.

3. **Endpoint Security**
    a. External computers that are used to administer university resources or access sensitive information on university resources must be secured. This includes patching (operating systems and applications), possessing updated anti-virus software, operating a firewall and being configured in accordance with all relevant university policies/procedures. The university will verify that external computers are compliant with university security standards.
    b. Use of the following tools and practices are required on all University remote computers, non-Georgia Southern and personally owned computers:
        i. Antivirus software, with daily updates enabled and full system scans enabled.
        ii. Patched with the latest approved security patches, including those for Web Browsers.
        iii. Windows Update must be enabled and set to auto-install updates.
        iv. A secure and encrypted remote-control application.
        v. VPN software installed and used whenever the remote control application is being used.
        vi. Personal firewall.
        vii. A technology or process for detecting and removing spy ware.
        viii. Users of remote access services (VPN) will permit the university to install an agent on their computer for verification of current AV updates and operating system patches. The university assumes no liability in the interruption of network service or resulting "problems" experienced by the user as a result of doing so.

4. **Technical Services supported tools:**
    a. Individuals must coordinate with their departmental technical representative to determine which specific vendors' tools to use and to obtain information on how

the tools will be supported. To receive technical support, staff members must use the listed tools and run Windows XP, Windows 7, MAC or Linux operating system.

i. Cisco VPN Client - provides a secure connection between the remote computer and the university campus.
ii. Microsoft Forefront AV/malware protection
iii. Microsoft Remote Desktop

5. **Third Party Remote Access:**
   A third party is any Georgia Southern authorized contractor, vendor and non-Georgia Southern authorized persons using any device connecting to the Georgia Southern network and/or through any other network service.

   a. Third party users must have a Georgia Southern University sponsor to complete the VPN request form
   b. Third parties must adhere to all University policies and standards to ensure University resources are adequately protected.
   c. Remote access privileges to third parties must be reviewed per the time restrictions on the initial VPN request or upon change of status of the third party.

6. **Responsibilities**
   The CIO or his/her designee is responsible for ensuring the implementation of the requirements of the Remote Access standard. Employees who violate this standard will be subject to disciplinary action up to and including termination of employment.

7. **Related Documents**
   Acceptable Use Policy
   Remote Access Policy
   Data Stewardship and Classification Standards