3.5 Remote Access Policy

POLICY:

Remote connection to Gordon College's computer systems, networks, and data repositories will be permitted only through secure, authenticated, and centrally managed access methods.

Rationale:

Increases in non-traditional teaching methods and the increased mobility of faculty, staff and students has made remote access to centralized College assets increasingly important. Opening uncontrolled or unsecured paths into any element of the College network or internal computer systems presents additional risk to the entire College infrastructure. Establishing policy centrally and issuing standards from a central authority allows a minimum number of penetrations of the security of the network while still allowing flexibility in the actual remote connection technology used.

Computer Services, as the manager of the institutional infrastructure, will establish and publish standards. College and Departmental contacts will assist with monitoring compliance with the standards by their respective users. Changes to standards when necessary will be communicated to the College by Computer Services.

Access to single host systems:

Remote access to single equipment hosts (i.e. departmental servers, WEB hosting equipment) is permitted by following these standards:

- Departmental host may provide dial-up modem service ONLY IF that service is limited exclusively to College members and the host prevents connection to the Gordon College network for those dial-in users.
- WEB hosting servers may provide anonymous or authenticated access to pages ONLY IF the service host prevents an onward unauthenticated connection to the Gordon College network.

In both instances, departments are responsible for hosts/servers operating within their departments.

Administration/Authentication:

The administration and authentication system for remote access will be centrally managed.

Affiliates are personnel that are not faculty, staff or students at the College who require remote access privileges. Affiliations may be requested by faculty and staff and are subject to an approval process.

Authentication for remote access will be strong. Passwords must meet minimum requirements as documented in College security policies.

Anonymous Interaction:

With the exception of web servers, electronic bulletin boards, or other systems where all regular users are anonymous, users are prohibited from remotely logging into any Gordon College system or network anonymously (for example, by using "guest" user-IDs). If users employ systems facilities which allow them to change the active user-ID to gain certain privileges, they must have initially logged-in employing a user-ID that clearly indicates their identity.

Anti-Virus and Firewall Protection:

External computers or networks making remote connection to College internal computers or networks should utilize an active virus scanning and repair program and an active personal firewall system (hardware or software).

Disclosure of Systems Information:

The internal addresses, configurations, and related system design information for Gordon College computers and networks is confidential and must not be released to third parties who do not have a demonstrable need-to-know such information. Likewise, the security measures employed to protect College computers and networks are confidential and should be similarly protected.

Failure to Authenticate:

All systems accepting remote connections from public network connected users must temporarily terminate the connection or time-out the user-ID following a sequence of several unsuccessful attempts to log-in.

Initiating Remote Sessions:

Instruction and assistance on initiating remote access sessions will be developed and offered by Departmental contacts in coordination with Computer Services.

Management Consoles and Other Special Needs:

Users requiring access for “out of band” management or special needs must register usage with Computer Services Department. Any server that grants network access must authenticate each user by a unique identification with password.

Remote Access to College Information:

Systems that contain confidential student, personnel and financial data will be available for off-site remote access only after an explicit request is made and approved by the data steward for the target system. Access will be permitted through a centrally managed virtual private network (VPN) that provides encryption and secure authentication

Time-Out:

All systems accepting remote connections from public network connected users must include a time-out system. This time-out system must terminate all sessions that have had no activity for a specified period of time.