

## 3.6 Internet Services (Server) Registration Policy

### **POLICY:**

All devices connected to the Gordon College network that are intended to “serve” information to on or off campus users must be registered with Computer Services.

### **Rationale:**

The rising frequency of security incidents involving network-attached devices significantly increases the probability of major disruptions to the internal computer systems of the College. Current server technology is easily implemented but the platforms if not properly configured provide an extremely vulnerable and high risk opportunity for exploitation and significant damage to other connected devices, other external devices, and other users. Registration of all such serving devices with accompanying procedures for verifying security configurations will significantly reduce the potential for this type of damage and also greatly shorten the time needed to identify and isolate equipment which has been inadvertently compromised. Additionally, care taken in build and deployment of serving devices provides a greater level of protection to other devices connected to the network. Establishing policy centrally and issuing standards and utilities from a central authority allows for rapid incident response and continuous update of protection methods.

### **Compliance:**

Chairs and Vice Presidents are responsible for monitoring compliance with this policy and associated standards by: (1) directing the registration of machines within their respective organizations that meet the standard definition of servers; and (2) directing reviews of, and action on, reports on unregistered serving devices connected to the College network that are generated by Computer Services.

### **Definition of Servers:**

Typically, servers are machines that have intentionally been set up to provide services to others on campus or the Internet. These provided services could include Web (http) servers, FTP servers, file sharing servers, etc. Most of these services are not typically offered by end-user workstations. However, if an end-user workstation has installed or turned on web server, FTP server, etc. services, this machine would be required to register as a serving device.

### **Server Registration:**

As a minimum, Computer Services must be provided the following information on each device currently or intended to be attached to the College network for the purpose of “serving” information either on or off campus:

- Brand of hardware platform
- Operating system version
- Equipment MAC address
- Requested DNS name
- Assigned or requested IP address

- Person responsible for management of the device (including phone number and email address)
- Device physical location
- Internet services being offered by the platform
- Security Protection measures applied to the device

As a continuing activity associated with normal network management, Computer Services will periodically scan for network-connected devices. Any unregistered serving devices found during these scans will be isolated from the network until proper registration is accomplished. When it has been determined by the College Information Security Officer that a security incident or compromise has occurred, failure to have accomplished registration will result in deactivation of network ports associated with the serving device.

#### **Server Security Audits:**

Administrative departments are responsible for developing and administering their own local procedures for initial verification of server security configuration as well as for ensuring that updated security patches are applied to serving devices within their respective organizations. Assistance from Computer Services is available for initial system verification and for periodic scans of systems. Computer Services will provide minimum requirements for server configurations. Failure to meet these minimums will result in the serving device being isolated from the network.