Policy Summary

Authorized users of Georgia State University computer systems networks and data repositories may be permitted to use wireless technology to connect to those systems, networks or data repositories for the conduct of university-related business only through authenticated and centrally managed access methods.

Full Policy Text

Authorized users of Georgia State University computer systems networks and data repositories may be permitted to use wireless technology to connect to those systems, networks or data repositories for the conduct of university-related business only through authenticated and centrally managed access methods.

Administration of Policy

Mandating Authority:
Provost

Responsible Office(s):
Information Systems and Technology, 13th floor, Commerce Building, 3-4357

Responsible Executive(s):

Policy History

Approving Body: Other

Rationale or Purpose

Increase in the availability of wireless technology and the ease of deployment has significantly increased the potential for unauthorized access to university information systems. Deployment of the Student Wireless system established a framework for authenticated access across the campus. Establishing policy centrally and configuration and management of access points by a central authority allow a minimum number of penetrations of the security of the network.

Additional Information

Access Method. All access through wireless access points connected to the university network
infrastructure (regardless of duration) will be by Virtual Private Network (VPN) tunnel or Wireless Gateway, and authentication using Novell userid and password. Mobile access points will be permitted to operate only from network ports configured by Information Systems and Technology (IS&T) for this purpose. Existing local procedures for access must comply no later than June 30, 2004.

**Configuration, Installation, and Management.** All fixed wireless access points connecting to the university network infrastructure will be configured, installed and managed by IS&T. IS&T will provide periodic information to the university community on approved vendors and models of access points. Existing access points must, as a minimum, provide 802.11b service and be configurable to block broadcast of SSID. Non-compliant access points must be replaced no later than June 30, 2004.

**Unauthorized Access Points.** IS&T will periodically check the campus for unauthorized fixed and mobile access points, immediately disable the network ports supporting those access points and advise the operating department of necessity to comply with this policy.

Originally approved and made effective by the Provost January 5, 2004

**Additional Helpful Resources**