Allegany College of Maryland

WIRELESS NETWORK SECURITY POLICY

Adopted date 1/19/2008
Revised Date 6/17/2022
Approved by Board of Trustees 1/19/2008
Implementation 1/19/2008
Type of Policy: Operational

BACKGROUND AND PURPOSE

This policy has been constructed to establish security standards for the college Wireless Network and advises Students, Faculty, Staff, Guests, and Visitors on acceptable wireless network access methods.

College wireless network systems and their uses are governed by college policy as well as federal, state and local laws. Individuals who inappropriately or illegally use college wireless network systems and resources may be subject to all applicable college and legal penalties for such misuse.

Access to and use of the college's wireless network systems are privileges granted solely to Allegany College of Maryland students, faculty, staff, and those with special accounts. These privileges can be modified, limited, extended, or revoked at the discretion of the College with or without prior warning or consent.

POLICY

I. SCOPE OF THE POLICY

This policy establishes security standards for college-wide wireless network systems and provides guidelines for using wireless network resources at Allegany College of Maryland.

II. POLICY STATEMENT

College wireless network systems are designated as official academic research and college business tools. Alternate uses may be restricted or prohibited at the discretion of the College, especially when these uses conflict with or interfere with academic and administrative functions. Users of College wireless network systems must adhere to policies and governance as established in the Allegany College of Maryland Technology Resources Policy.

The Information Technology department will routinely monitor wireless network health. Monitoring includes the scanning for and disabling of rogue access points. The Information Technology department reserves the right to disable access points and wireless network services with or without prior warning or consent. The college makes no claim or guarantee on the security of data transmitted on college wireless network systems. In all circumstances, users of college wireless network systems assume all data is transmitted in clear text and should take necessary actions to secure data in transit.

III. Access to College Wireless Network Systems

An individual shall only use the network access credentials assigned to them. Students who are also employees of the College shall have access to faculty/staff wireless network systems. Faculty and staff access to College wireless network systems shall be granted at the start of employment and shall be revoked at termination of employment. Users may access faculty/staff wireless network systems using only the communications tools provided by the College. Visitors to the college (including the general public) are permitted to use the guest ("ACOM-Guest" service set identifier or "SSID") to access the College wireless network system.

IV. Restricted Uses of College Wireless Network Systems

Use of College wireless network systems for personal or financial gain is prohibited. Use of College wireless network systems to capture, monitor, listen, retransmit, or otherwise intercede network traffic is prohibited.

V. Student Wireless Network Access

Students actively enrolled in credit courses may access Wireless Network systems designated for student use. Access to the student Wireless Network is available by association to the ACM Service Set Identifier ("SSID").

Students must register associations to the student Wireless Network through authentication of a username and password. Student devices associated to the ACM SSID are required to be fully patched and have adequate antivirus installed. Students are responsible to maintain updates as required. The college reserves the right to quarantine, suspend, or otherwise disable network access to student devices found to pose a threat to network security or stability with or without prior warning or consent.

VI. Faculty/Staff Wireless Network Access

College faculty and staff members may access Wireless Network systems designated for general use. Access is available by association to the ACM Service Set Identifier ("SSID"). College faculty and staff members must register associations to the general Wireless Network through authentication of ACM username and password.

Faculty and staff owned devices associated to the ACM SSID are required to be fully patched and have adequate antivirus installed. Faculty and staff are responsible to maintain updates as required. The college reserves the right to quarantine, suspend, or otherwise disable network access to faculty-owned and staff-owned devices found to pose a threat to network security or stability with or without prior warning or consent.

College faculty and staff members may access Wireless Network systems designated for faculty/staff use using only college-provided wireless devices. Access to the faculty/staff Wireless Network is available by association to the ACM Service Set Identifier. College faculty and staff members must register associations to the faculty/staff Wireless Network through authentication of ACM username and password.

College-owned wireless devices associated to the ACM SSID are required to be fully patched and maintained by the Information Technology department. Faculty and staff are responsible to bring wireless devices to the IT Helpdesk for configuration and routine maintenance.

The college reserves the right to quarantine, suspend, or otherwise disable network access to college-provided wireless devices found to pose threat to network security or stability with or without prior warning or consent.

VII. Guest/Special Account Wireless Network Access

With respect to Wireless Network Access, the college designates the following individuals as college guests:

a) Vendors and consultants executing existing college contracts
b) Vendors and consultants conducting planned informational and sales consultations
c) Presenters, lecturers, and speakers facilitating college-sponsored events
d) Named individuals representing organizations facilitating college-sponsored events or as part of a college-sponsored partnership.

College guests and those with special accounts may access Wireless Network systems designated for guest use. Access to the guest Wireless Network is available by association to the ACM SSID. College guests must register associations to the guest Wireless Network through authentication of assigned credentials. Credentials are provided by the IT Helpdesk after review and approval. Requests for guest credentials must be submitted at least one business day prior to the date of intended use. Devices associated to the ACM SSID are required to be fully patched and have adequate antivirus installed. College guests are responsible to maintain updates as required.

The college reserves the right to quarantine, suspend, or otherwise disable network access to guest devices found to pose a threat to network security or stability with or without prior warning or consent. The college reserves the right to expire or terminate network access to guest devices with or without prior warning or consent.

VIII. Enforcement

Technology resources and their uses are governed by College policy as well as federal, state and local laws. Individuals who inappropriately or illegally use College technology services and resources may suffer all applicable College and legal penalties for such misuse.

IX. Administration of Policy

The office of the Dean of Information Technology, in consultation with The Vice President of Finance and Administration, shall be responsible for maintaining this policy.

X. Changes

Substantive changes to this policy require approval by the Board of Trustees; editorial changes, title/position changes, and/or changes to its implementation procedures may be made as required by federal or state mandate and/or institutional need with timely notice to students and employees.