CSM Wireless Policy

1.0 Purpose

This policy prohibits access to College of Saint Mary (CSM) networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy are approved for connectivity to College of Saint Mary's networks.

2.0 Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of College of Saint Mary's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to College of Saint Mary’s networks do not fall under the purview of this policy.

3.0 Policy

3.1 Register Access Points

All wireless Access Points / Base Stations connected to all internal networks must be approved by the Director of Information Services. These Access Points / Base Stations are subject to periodic penetration tests and audits.

3.2 Approved Technology

All wireless LAN access must use CSM-approved vendor products and security configurations.

3.3 Encryption and Authentication

All computers with wireless LAN devices must utilize a CSM-approved encryption configured to route all unauthenticated and unencrypted traffic to a separate logical network from our production network. To comply with this policy, all implementations must support and employ strong user authentication which checks against an external database such as RADIUS, Active Directory (Windows Internet Authentication Service) or something similar. Furthermore, each user is required to use the user account that has been assigned him or her. Under no circumstances shall generic logons be allowed to gain access to the network through wireless means.

3.4 Setting the SSID(s)

The SSID(s) shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

4.0 Enforcement

Any student found to have violated this policy may be subject to disciplinary action, up to and including expulsion. Any employee found to have violated this policy may be subject to disciplinary actions up to and including termination.

5.0 Definitions

Terms	Definitions
RADIUS	Remote Authentication Dial-In User Service – A method of authenticating a user by sending username and password to a centralized server
SSID	Service Set Identifier – Used as the logical name of a wireless access point/base station.
User Authentication	A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

6.0 Revision History