Connors State College
Information Technology Systems
Wireless Communication Policy

1.0 Overview

**Summary:** This policy governs the use of the wireless network(s) on our campuses.

Wireless implementations are a benefit to Connors State College, its’ faculty and staff, and its’ students. Maintaining these implementations can be a tedious process and the use of these implementations is a necessity. Seeing that these implementations remain operational and within requirements we have sought to establish this wireless communication policy.

2.0 Purpose

This policy prohibits access to Connors State College networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by CSC IT Systems Department are approved for connectivity to Connors State College networks.

3.0 Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of Connors State College'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 Connors State College’s data networks do not fall under the purview of this policy.

4.0 Policy

4.1 Register Access Points and Cards

All wireless Access Points / Base Stations connected to the corporate network must be registered and approved by the CSC IT Systems Department. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with CSC IT Department.

4.2 Approved Technology

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

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Revision History
7.0 Definitions

<table>
<thead>
<tr>
<th>Terms</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Authentication</td>
<td>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.</td>
</tr>
</tbody>
</table>
I certify, by signing below, that I have read and understood the policies mentioned within this document and I will abide by them follow the guidelines set forth herein.

______________________________
Print Name

______________________________        ________________
Signature        Date

Connors State College
Information Technology Systems

Ph: 918.463.6323
Fax: 918.463.6316
it@connorsstate.edu