

## **Bicentennial Inn Security Statement**

In providing this Security Statement, we want you to be better informed about the security limitations and features of our Bicentennial Inn Wireless service.

Our wireless network is based on wireless local area networks ("WLANs") that use evolving technology based on the IEEE 802.11b and IEEE 802.11g standards. These WLANs are not inherently secure. We therefore cannot guarantee the privacy of your data and communications while using the wireless service. However, we support customer-provided security solutions, such as virtual private networks ("VPNs"), encryption and personal firewalls, and have recently deployed the new 802.1x/WPA (Wi-Fi protected access) security technology to better protect your wireless communications.

### **802.1x/WPA**

For authentication purposes, if used, our 802.1x/WPA solution encrypts your wireless transmissions from your laptop, PDA (personal digital assistant) or other Wi-Fi device, through our access points at the wireless location to our login servers. Once you are authenticated and authorized, WPA encrypts your data traffic, including user names, passwords and credit card information, when it is transmitted wirelessly (or "over the air") from your Wi-Fi device to the installed access points. The encryption helps protect against unauthorized interception of your data while it is transmitted "over the air" between your device and our access points. It also helps to mitigate against session hijacking (the ability for unauthorized individuals to access Wi-Fi service for free using a customer's session). It does not, however, protect your data once it is transmitted over the Internet. Once you connect to the Internet, it is your responsibility to provide proper encryption, such as a VPN or the use of websites that offer secure socket layer ("SSL") technology.

### **Additional Information**

Bicentennial Inn strongly recommends you take measures to secure your Wi-Fi devices and Internet communications. We encourage and support many customer-provided security solutions, such as VPNs, personal firewalls and the use of websites that provide SSL encryption for your data. It is your responsibility, however, to take these precautions and provide security measures best suited to your situation and intended use of the service. We do not currently provide these solutions and cannot guarantee or otherwise be responsible for their effectiveness. Please note that appropriate safeguards should be used for any type of wireless technology or Internet access via any service provider. If you are interested in learning more, a few sources of additional information are: the National Infrastructure Protection Center's website at <http://www.nipc.gov/publications/nipcpub/bestpract.html> and CERT's website at [http://www.cert.org/tech\\_tips/home\\_networks.html](http://www.cert.org/tech_tips/home_networks.html).

Please keep in mind that this statement only addresses our wireless service and is limited in scope. It does not and is not intended to cover all types of network, device or Internet security issues or risks. For example, wired and wireless networks and devices (such as PDAs, desk top and laptop computers, and servers) may be susceptible to viruses, Trojan horses, and denial of service attacks. We encourage you to use other resources, such as those found on the Internet, and at libraries or in bookstores, for comprehensive information concerning these and other security risks and issues. We may update this Security Statement from time to time. Please check regularly for updates.