547.18 What standards apply to Class II gaming systems utilizing wireless player interfaces?

(a) If a player interface utilizes wireless technology to connect to any part of the Class II gaming system, the wireless gaming system must:

1. Physically locate system components including but not limited to wireless access points (AP), mobility controllers, and wireless gaming servers in secured areas not easily accessible to the public;

2. Disable all exposed network connectivity ports (Ethernet, USB, etc.) on the player interface, if applicable;

3. Utilize an independent network for the wireless gaming system;

4. Suspend the wireless player interface device from game play while the wireless player interface is located outside of the approved gaming area or loses connectivity with the wireless gaming system;

5. Require the wireless player interface to re-authenticate before resuming play at the last known game state prior to being suspended when the wireless player interface re-enters the approved gaming area or re-establishes connectivity with the wireless gaming system;

6. Implement a time period which is configurable for re-authentication;

(b) *Wireless communication with a player interface.*

1. Wireless communication between a gaming system and a player interface must be conducted using a method that securely links the gaming system and the player interface and authenticates both the player interface and the gaming system as authorized to communicate over that link;

2. A wireless player interface shall be sufficiently isolated within the gaming system so as to restrict the player interface from unauthorized access to system components;

3. A wireless player interface must be designed or programmed such that it may only communicate with authorized gaming systems;

4. A wireless player interface must employ encryption and strong user authentication methods;

5. A wireless gaming system must utilize a stand-alone firewall, which must isolate the access points (AP) from other network components;

6. A wireless gaming system must provide a printable report of failed network access attempts, including time and date stamp, device name, and hardware identifier of all devices requesting access to the network;
(7) A wireless gaming system must provide the capability for the administrator to disable the player interface at any time.

(c) Firewall Audit Logs. The firewall application must maintain an audit log of the following information and must disable all communications and generate an error event if the audit log becomes full:

(1) All changes to configuration of the firewall;

(2) All successful and unsuccessful connection attempts through the firewall; and

(3) The source and destination IP Address, Port Numbers and MAC addresses.