Wireless Technical Document

If a casino decides to use a wireless WLAN as part of their overall network, the Division recommends the casino use the following best practices. WLANs should be implemented with strong security controls. It is the casino's responsibility to install, maintain, and monitor the WLAN. Once the data is written to the gaming system's database, a copy of the gaming data is permitted across the WLAN. This includes results from queries, reports, or copies of the database itself. It is the casino's responsibility to ensure the security of all data traveling in the WLAN.

Security requirements that must be met include authentication and encryption. Other security requirements that should be met include monitoring, topology and incident response.

Physical Security

All WLAN components such as access points, wireless management systems, firewalls and Intrusion Detection systems (IDS) must be physically secure. Access points must be mounted using tamper proof mounting hardware in an area that does not allow for easy physical access or secured in a locked cabinet or room. The other WLAN infrastructure components must be in a secured room that is locked all the time.

Logical Security

All default settings must be changed before implementation. Changes to the default settings must be documented.

Parameters that should be changed include but are not limited to:

- Default Pre-shared key (1.2a)
- SSID (1.2b)
- SNMP community strings (1.2c)
- Encryption Keys (1.2d)
- Passwords (1.2E)
- Disable any unnecessary ports, protocols, broad casts or other options (1.2f)
- Change clock settings to synchronize with the casino's time system (1.2g)
- Set a session timeout (to prevent hijacking of abandoned authentication sessions(1.2h)
- Disable WPS (1.2i)

For more information on default settings please refer to the logical security document.

The WLAN must be segmented from the environment that contains gaming data. This segmentation must be done with a firewall that has stateful packet inspection. Virtual local area networks (VLAN) do not segment the wireless network appropriately and are not approved. In addition to the firewall there should be a system that monitors and prevents unauthorized access by inspecting the header and payload of each packet. This is typically done by an Intrusion Detection/Intrusion Prevention system (IDS/IPS).

By default all traffic in and out of the WLAN should be denied. Authorized traffic should then be explicitly allowed to pass through the WLAN. All traffic from the WLAN should be logged by the device. All logs from WLAN infrastructure equipment should be reviewed at least weekly. Evidence of the review includes initials, date, and gaming license number of the reviewer. A log monitoring system that alerts the administrator to suspicious activity does fulfill the log review requirement. Should problem events be identified that did not trigger an incident, the event should be logged and remediated using the usual helpdesk procedures for remediating problems.

Validation of logical security configurations should be tested annually. The Division recommends the validation include penetration testing from within the network as well as from outside the network. The results should be documented and reviewed by management. Evidence of the review includes initials, date, and gaming license number of the reviewer.

All WLAN components should have security patches installed no later than 30 days after release.

Authentication

Authentication requirements include:

- Using strong passphrases – Strong passphrases should include letters, numbers and special characters if possible.
- Changing default passwords – There are typically one or more accounts that are established by default from the manufacturer. The most common is an administrator account. Passwords should be changed before the wireless device is implemented.
- Minimize the number of people who have access to accounts with elevated privileges.
- Accounts with elevated privileges should have their passwords change at intervals no longer than 90 days. Only employees with elevated privileges are allowed access to WLAN.
- The authentication routine should be encrypted.
- The change must be documented.

- Devices that timeout should authenticate again.

For more information on account management please refer to the logical security document.

Encryption

Because cryptographic strength is crucial to a secure WLAN, old encryption versions become a risk and should be updated. To mitigate this risk it is recommended that the encryption version is in line with IT best practices and industry standards, for example National institute of standards and technology (http://www.NIST.gov). Currently the most common implementations are WPA or WPA2 with AES encryption. It is recommended that AES-256 bit encryption should be used.

Key management is crucial to security in a WLAN. Pre-Shared keys must be managed, documented and changed whenever there is a security incident involving a breach to the wireless network, a person with knowledge of the keys has left, or at least annually.

Monitoring and Incident Response

The casino should monitor the WLAN for suspicious activity such as repeated unsuccessful login attempts, blocked intrusion attempts or unauthorized devices trying to connect to the WLAN. Common equipment for monitoring the WLAN includes Firewalls, Intrusion detection/ Intrusion prevention systems, Network Policy servers and Wireless Management Servers. These systems should be able to automatically report suspicious activity to the administrator. In order to remediate or justify the activity, the administrator should begin an investigation within a reasonable time frame. The activity should then be documented.

If the suspicious activity is an actual attack on the WLAN which causes a disruption in the collection, accuracy, integrity, or availability of the production environment, the casino should begin the troubleshooting process. The casino should take immediate action to mitigate the attack.

Topology

The WLAN must be documented in a network diagram. The map must include all components of the WLAN as well as the path to the wired network. The data moving in the WLAN must be documented within the diagram. The map must include near field communication protocols (like Bluetooth) except for input devices on endpoint workstations such as wireless keyboards and/or mice. The network map must be updated when there is a change to the network.

Casinos with the same ownership or casinos with an unattached business office may establish a wireless bridge. The casino must follow all rules for segregation of data, for example ticketing data. The wireless connection between the two properties should use grid antennas and follow all of the other security points outlined in this document.

Glossary

AES	Advance Encryption Standard
Antennas	
Grid(parabolic)	Directional antenna
Encrypt(ion)	Encipher or Encode
Firewall	Device or software that prevent unauthorized access by outside computer users
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
SNMP	Simple network Management Protocol
SSID	Service set Identifier
VLAN	Virtual local area network
WLAN	Wireless local area network
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup