ILLINOIS GAMING BOARD
MINIMUM INTERNAL CONTROL STANDARDS
SECTION A - GENERAL AND ADMINISTRATIVE

TABLE OF CONTENTS

General

1. In addition to complying with these Minimum Internal Control Standards (MICS), Owner Licensees are required to comply with the Illinois Gambling Act and Illinois Gaming Board Adopted Rules.

2. In addition to written procedures, flowcharts, although not required, may be included in the ICS. Flowcharts must mirror the written procedures, however if there is a difference noted, the written procedures must be the procedures followed.

3. These MICS include general names for positions and forms. Specific titles and form names must be included in the Owner Licensee's ICS.

4. The term "non-gaming employee" means a member of the security, cage or accounting departments.

5. The lowest job title of that department with the authority for that duty must be listed in the ICS procedures. Employees with higher authority within the same department may perform these duties, except where specifically noted in the ICS. When a higher job title of that department performs the duties of a lower job title of that department, he/she may not then perform verification of his/her own work.

   A lower job title may be assigned the job duties of a higher job title within the same department for the gaming day, provided that the assigned job title is within the same IGB Occupational License Badge Level. An employee temporarily working in the higher job title may not perform verification of his/her own work. Once assigned to the higher job title, the employee cannot return to his/her lower job title for the rest of the gaming day. Any lower job title elevated to a supervisory job title cannot accept tips or gratuities while performing the job duties of the higher job title.

6. Sensitive areas are those areas that management or the IGB considers sensitive to the Owner Licensee's operation and therefore require strict control over access (e.g. pits, count rooms, cage, and surveillance rooms).

The ICS must include:

1. Organizational charts for the Owner Licensee, from the Board of Directors (or equivalent) on down and for all gaming related departments including live games, electronic gaming devices, drop and count, casino cashiering and credit, internal audit, casino accounting, surveillance, security, marketing, purchasing and contract administration, admissions and management information system;

2. A detailed description of each position shown on the organizational charts which includes:

   a. Duties and responsibilities;
   b. Immediate supervisor;
   c. Positions directly supervised;
   d. Signatory ability, including alternate procedures in cases in which the required signator is unable to perform his duty; and
   e. Access to sensitive assets and areas; and

3. Type of training employees receive regarding the Illinois Gambling Act, IGB Adopted Rules and the Owner Licensee's ICS.

Owners, Board of Directors or officers/executives must not have unaccompanied access to sensitive areas. If a reason exists for such person or persons to access a sensitive area, the IGB Docksite Supervisor/Agent must be notified and give permission prior to access. Security must accompany such person or persons while in a sensitive area. Security must obtain prior IGB approval before entering surveillance.

Management Information Systems (MIS)

The Owner Licensee must provide the IGB Administrator or designee with a topology and a description of each management information system and how each of the systems, (e.g. casino management system, Computer Monitoring System, cashless wagering system, slot information system and Voucher System) are individually distinguished and accessible in respect to how the systems interact with one another in the computer environment that they are housed (e.g. virtualized, physical, etc.)

The ICS must include a description of all management information system(s) used that impact gaming operations, ensuring that procedures are established to:

1. Control the ability to access computer programs and equipment at each level;

2. Secure systems by user access that offer segregation and definition of duties and limits of authority, which are determined by casino management. User accounts and passwords must be issued and controlled by a System Administrator or their equivalent in the MIS department;

3. Generate and archive a thirty day unalterable digital log of user access and security incidents. The IGB Supervisor/Agent and the MIS department must be notified immediately of any event and/or condition that has the potential to impact the security of the MIS that may result from intentional or unintentional actions;

4. Assign rights and privileges to each user, including:

    a. allowance for the secure administration of user accounts to provide an adequate segregation of duties;
    b. use of appropriate access protocols to restrict unauthorized users from viewing, changing or deleting critical files and directories;
    c. assignment and retention of an updated matrix of the rights and privileges of each user;
    d. utilizing strong passwords that include the minimum number of characters required and any password complexity standards required (e.g., combination of letters and numbers). The ICS must include a description of the minimum strong password requirements, i.e., alpha, numeric; symbols, uppercase, etc.
    e. monitoring and recording of all logins while employing system lockout parameters;
    f. expiration of passwords;
    g. establishment of terminal or system inactivity parameters, at which time the user(s) must be required to re-authenticate access;
    h. ensuring vendor/manufacturer supplied default passwords are changed prior to system implementation;

i. establishment of a maximum number of times a user can attempt to enter their password in order to gain access to the system and lock out features after the maximum number of times has been exceeded;
j. updating or changing of user information (passwords, names, terminations, etc.); and
k. notifying MIS staff of employee terminations or reassignments;

5. Review security violation reports;

6. Address network security, including:

a. reviewing firewall rule settings and recertifying ingress/egress filters;
b. segmenting networked gaming systems from network segments accessible from the Internet;
c. monitoring changes to router configurations;
d. implementing and monitoring an intrusion detection system;
e. implementing and monitoring anti-virus software;
f. ensuring all patch levels are current; and
g. securing networking;

7. Back-up files and monitor for successful completion of the back-up process;

8. Test and document system backup and recovery procedures; including if a catastrophic failure occurs and the system (s) cannot be restarted, it must be possible to reload the system (s) from the last viable backup point and fully recover the contents of the back-up;

9. Protect files (offsite storage of back-up files). The IGB Administrator or their designee and the IGB Docksite Supervisor must be notified in writing of the offsite storage location and any changes in the location;

10. Develop, maintain, and test a Disaster Recovery Plan including all critical applications and vendor purchased applications;

11. Safeguard software and equipment, including

a. limiting access to computer software and equipment (restricted access, locked doors);
b. providing controls over cooling, humidity, and water;
c. providing a back-up power supply including maintenance and testing schedules; and
d. Fire Prevention/Mitigation measures;

12. Change control procedures for new or upgraded hardware and software including;

a. separate environments for development, test and production;
b. user acceptance testing and documentation of testing results;
c. separation of individuals responsible for moving changes into production and development staff; and
d. emergency changes;

13. Notify and obtain approval of the IGB Administrator of proposed changes, (including any management information system maintenance changes) to management information systems, (e.g. casino management system, Computer Monitoring System, cashless wagering system, slot information system and Voucher System). The MIS Department

must provide a written report to the IGB Administrator detailing the proposed changes; and

14. Compare computer generated information affecting gaming tax revenues through physical count, management analysis and other methods.

Remote Access

Remote Access to an Owner Licensee's ("Owner Licensee" or "Casino") Computer Monitoring System, Voucher System and cashless wagering system ("Critical Gaming System(s)") is prohibited unless the IGB Administrator has approved internal controls that specifically address Remote Access procedures. These procedures must provide, at a minimum, that:

1. Remote Access to a casino's Critical Gaming System(s) must only be approved by authorized and licensed casino MIS employees listed in the ICS.

2. Remote Access to a casino's Critical Gaming System(s) must be granted only on an as needed basis to upgrade, update, repair, alter or maintain the Critical Gaming System(s).

3. Remote Access to a casino's Critical Gaming System(s) must only be granted to either an authorized licensed Supplier, an authorized licensed casino MIS employee, or an authorized MIS employee of a casino's key person parent entity. Remote Access by an authorized licensed Supplier, an authorized licensed casino MIS employee or an authorized MIS employee of a casino's key person parent entity must only be allowed using a computer issued by the licensed Supplier, casino or its key person parent entity using a secure encrypted connection identified in the ICS.

4. A Remote Access authorization request form must be completed prior to each Remote Access session to a casino's Critical Gaming System(s). Notwithstanding the foregoing:

    a. Where necessary and practicable under immoderate circumstances, an authorized licensed Supplier or an authorized MIS employee of a casino's key person parent entity may be granted Remote Access for an extended period of time not to exceed 7 days with a single Remote Access authorization request form completed prior to the beginning of the extended remote access session; and

    b. Where necessary and practicable under the circumstances, an authorized licensed casino MIS employee, as listed in the ICS, may be granted Remote Access for an extended period of time not to exceed 30 days with a single Remote Access authorization request form completed prior to the beginning of the extended remote access session.

    c. The ICS must describe procedures for the preparation, required signatures and maintenance of the Remote Access authorization request form(s).

5. For Critical Gaming System(s) which can be accessed remotely, the ICS must specifically address Remote Access procedures and include, at a minimum:

a. The method and procedures used in establishing user accounts and passwords to allow an authorized licensed Supplier, an authorized licensed casino MIS employee or an authorized MIS employee of a casino's key person parent entity access to the system through Remote Access; and

b. The personnel involved and procedures performed to enable the method of establishing Remote Access connection to the system when an authorized licensed Supplier, an authorized licensed casino MIS employee, or an authorized MIS employee of a casino's key person parent entity requires access to the system through Remote Access.

6. Remote Access to a casino's Critical Gaming System(s) must require safeguards to ensure the integrity of the system(s).

a. Remote Access connections to a casino's Critical Gaming System(s) must employ Two-Factor Authentication (T-FA) prior to opening a session (e.g., username and password, ID card, or biometrics). The specific method used must be listed in the ICS. The ICS must also include procedures for periodic verification of user access with the authorized licensed Supplier, authorized licensed casino MIS employee, or authorized MIS employee of a casino's key person parent entity.

b. Remote Access to a casino's Critical Gaming Systems must be monitored by a current industry accepted system or application that can effectively monitor and log a remote user's activities while remotely accessing a casino's management information system(s). A detailed description of the methods in use must be included in the ICS.

c. Remote Access with any portion of the casino's Critical Gaming System(s) must use a secure encrypted connection (e.g., Virtual Private Network technology). A detailed description of the method used, including security measures, must be included in the ICS.

7. The Owner Licensee's Remote Access server for Critical Gaming System(s) must have policies in place to assess the remote user's computer to determine compliance with the Owner Licensee's security policies, such as having current anti-virus protection and security patches installed.

8. Remote Access to a casino's Critical Gaming System(s) must require that whenever Remote Access is not in use, Remote Access must be physically or logically (e.g., log-off, etc.) disabled to prevent access. The MIS department will review, at a minimum daily, all current Remote Access requests for authorized licensed Suppliers, authorized licensed casino MIS employees and authorized MIS employees of a casino's key person parent entity to ensure that open sessions are still in use. In the event that an open session is not in use, the MIS department must contact the Remote Access user to determine if the requested Remote Access has been completed, and if the requested Remote Access has been completed access will be immediately disabled.

9. For each Remote Access to a casino's Critical Gaming System(s), system audit records must be generated and maintained on the server or other secure system component. The records must include the following information pertaining to each Remote Access:

    a. The user ID, time and date of Remote Access;
    b. A record of programs transferred or changed;
    c. A record of all changes to the Critical Gaming System(s) made by the user; and
    d. The duration of Remote Access.

10. Remote Access to a casino's Critical Gaming System(s) may also otherwise be allowed with the prior written approval of the IGB Administrator.

11. Remote Access to a casino's non-Critical Gaming System(s), with the exception of the surveillance system, is allowed so long as that access does not and cannot communicate or otherwise interact with the Critical Gaming System(s).

12. Remote Access to an Owner Licensee's surveillance system is prohibited.

Voucher System Security

1. The System Administrator will ensure the following minimum functions are performed to control access to the Voucher System:

    a. Generate daily monitoring logs of security incidents and unusual transactions, and immediately notify or cause to immediately notify an IGB Agent and the MIS Department of critical security incidents and unusual transactions;
    b. Utilize encryption or password protection or equivalent security for files and directories containing critical or sensitive data. If encryption is not used, users must be restricted from viewing the contents of such files and directories, which at a minimum must provide for:

        i. the effective segregation of duties and responsibilities with regard to the system in the MIS Department; and
        ii. the automatic monitoring and recording by the system of access by any person to such files and directories; and

    c. Perform the following minimum functions to control system operations:

        i. validate the identity of those devices from which a transmission is received;
        ii. ensure that all data sent through a transmission is completely and accurately received; and
        iii. detect the presence of corrupt or instances of lost data and, as necessary, reject the transmission.

2. The System Administrator must:

a. Ensure that remote access be prohibited unless the IGB Administrator has approved internal controls that specifically address remote access procedures; and
b. Ensure that all voucher transactions are retained for the prior three years, either on-line or in a media approved by the IGB Administrator and capable of being restored to the Voucher System upon request.

3. The Voucher System must perform the following minimum functions to control the integrity of voucher system data:

a. Generate or cause to be generated a validation number for each voucher, either utilizing a unique algorithm, or by such other method approved by the IGB Administrator and the certification laboratory, which method must prevent the ability to predict the composition of any other validation number generated by the system;
b. Validate the data type and format of all inputs to critical fields and reject any corrupt data;
c. Provide for the automatic and independent recordation of critical data upon issuance of a voucher and redemption; and
d. Provide for verification of the information contained on a voucher presented for redemption and for the record of unredeemed vouchers to a source that separately records and maintains transaction data, or such other compensating procedure as approved by the IGB Administrator and the certification laboratory, which procedure must independently verify the accuracy of the validation number and value prior to redeeming the voucher.

4. The Voucher System must perform the following minimum functions to address business continuity:

a. Utilize data redundancy techniques that ensure system data preservation; and
b. Utilize environmental controls, such as uninterruptible power supplies, and fire and water resistant materials to protect critical data from natural disaster.

5. The MIS Department, Surveillance Department and/or the Security Department must immediately notify an IGB Docksite Supervisor/Agent of any malfunction that threatens the integrity of the Voucher System.

6. The Voucher System must not be capable of issuing or validating a duplicate voucher on demand.

7. Ensure that once the validation information is stored in the database, the data may not be altered in any way, without the alterations being captured and reported on the appropriate system logs.

8. Ensure that any device that holds voucher information in its memory must not allow removal of the information unless it has first transferred that information to the database or other secured component(s) of the Voucher System.

Problem and Underage Gambling

Licensees are to provide training to employees and information to employees and the public concerning problem, compulsive and underage gambling. The ICS must:

1. Provide for posting of information and the dissemination of information as provided in Section 13.1(a) of the Illinois Gambling Act;

2. State that the licensee is to develop procedures and training to assist patrons or others inquiring on behalf of patrons in gaining information about problem or compulsive gambling and treatment for problem and compulsive gambling;

3. State that the licensee is to disseminate, through training and other means, information to its staff regarding the nature of problem and compulsive gambling, and the licensee's policies concerning the identification of or assistance to persons with gambling problems. Similar training and information is to be provided concerning the prevention and detection of underage gambling; and

4. Specify the personnel to be trained and the types and frequency of training that will be utilized to maintain employee understanding of the licensee's policies and procedures regarding problem, compulsive and underage gambling.

Property Based Self-Exclusion Program

1. If a property based self-exclusion program is maintained by an Owner Licensee, establish procedures by which a patron can "self-exclude" himself or herself from the Riverboat Gaming Operation. The ICS must include the following:

    a. Procedures by which a patron's name and address is flagged on all mailing, marketing and promotional lists and databases so that he/she is removed from all services, including check cashing and credit, and promotional inducements offered by a licensee. Identify the employees of the Owner Licensee responsible for reviewing and effectuating the removal;
    b. Procedures for detecting persons on the property based self-exclusion list that have entered the gaming premises of a Riverboat Gaming Operation;
    c. Procedures for the removal of the property based self-excluded person from the gaming area;
    d. Procedures for maintaining the confidentiality of persons on the property based self-exclusion list that comply with the confidentiality requirements set forth in Subpart G of the IGB Adopted Rules; and
    e. If a property based self-exclusion program permits removal of a person's name from the property based self-exclusion list, provide procedures for removal of a person's name from the property based self-exclusion list including documentation of determinations made on a patron's request for removal of his/her name from the property based self-exclusion list. Identify the employees of the Owner Licensee responsible for reviewing and making determinations on all requests for removal from the property based self-exclusion list; and

2. A statement that the Owner Licensee will make available, in written form at each casino cage and credit location, information explaining these procedures.

IGB Statewide Voluntary Self-Exclusion Program

Owner Licensees are required to adopt policies and procedures outlined in the IGB Statewide Voluntary Self-Exclusion Program promulgated by the IGB in its Adopted Rules. The ICS must include a description of the IGB Statewide Voluntary Self-Exclusion Program policies and procedures, including the following:

1. Procedures by which a person's name and address is flagged on all mailing, marketing and promotional lists and all casino databases so that he/she is removed from all services, including check cashing and credit, and promotional inducements offered by a licensee. Identify the employees of the Owner Licensee responsible for reviewing and effectuating the removal;

2. Procedures for detecting persons on the IGB statewide voluntary self-exclusion list that have entered the gaming premises of a riverboat gaming operation, including:

    a. Procedures for immediate notification to the IGB Docksite Supervisor/Agent;
    b. Procedures for the inventory, in the presence of the IGB Docksite Supervisor/Agent, of all jackpots, chips in play or in plain view, vouchers and electronic credits in the possession or control of the self-excluded person;
    c. A description of the IGB statewide voluntary self-exclusion forfeiture form used to document the amount forfeited by the self-excluded person in 2.b above, including required signatures and distribution of the form. At a minimum, the distribution of the IGB statewide voluntary self-exclusion forfeiture form will be as follows: The original form will be forwarded to the IGB Statewide Voluntary Self-Exclusion Program Director by the General Manager within three days of forfeiture. Copies of the IGB statewide voluntary self-exclusion forfeiture form will be issued to: the casino cage, the security department, the IGB Docksite Supervisor/Agent and the self-excluded person;
    d. Procedures for the removal of the self-excluded person from the gaming area;
    e. The forfeited amounts associated with past-due support, if applicable, are to be deducted prior to any other remittance; and
    f. Procedures for remitting the forfeited amount to the duly registered charitable or governmental agency previously selected by the self-excluded person from a list of gambling support service and/or treatment providers approved by the Department of Human Services. The remittance amount to the duly registered charitable or governmental agency is net of amounts subject to past-due support; and

3. Procedures for maintaining the confidentiality of individuals on the IGB statewide voluntary self-exclusion list to be in compliance with the IGB Adopted Rules.

Signatures

1. All handwritten signatures must include the employee's first initial, last name and the last six digit numbers of their IGB occupational license number.

2. Electronic signature methods may be used if approved by the IGB Administrator. An electronic signature includes a non-handwritten unique means of identifying an individual based upon a system of administrative controls (such as passwords, personal

identification codes, and/or bar codes) or biometrics (such as retinal scans, voice prints, hand prints, and/or finger prints). An electronic signature must be the legally binding equivalent of a handwritten signature.

3. If electronic signatures are used, the ICS must include a description of the electronic signature system and its configuration, including:

   a. Procedures and controls designed to ensure the authenticity and integrity of electronic signatures and to ensure that the signer cannot readily repudiate the electronic signature as not genuine;
   b. The ability to generate complete copies of records with electronic signatures in readable format suitable for inspection, review, copying and printing; and
   c. Establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signature, in order to deter record and signature falsification.

4. Electronic signatures that are not based upon biometrics must employ at least two distinct identification components such as an identification code and password and be used only by their genuine owners. Licensees who use electronic signatures based upon use of identification codes in combination with passwords must employ controls to ensure their security and integrity, including:

   a. Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password;
   b. Ensuring that identification code and password issuances are periodically and properly checked, revised, and recalled (such as recall immediately after an employee's separation from employment);
   c. Following loss management procedures to electronically deactivate lost, stolen, missing or otherwise potentially compromised cards and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls; and
   d. Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes and detect and report in an immediate manner any attempts at their unauthorized use to system security.

5. Documents that employ electronic signatures must contain information associated with the signing that clearly indicate all of the following:

   a. The printed name of the signer as described in the ICS; and
   b. The date and time when the signature was executed.

6. Electronic signatures and handwritten signatures executed to electronic documents must be linked to their respective electronic documents to ensure that the signatures cannot be removed, copied or otherwise transferred so as to falsify an electronic document.

General Procedures for Promotional Coupons and Coupons for Complimentary Cash, Chips or Electronic Credits

The ICS must include the following:

1. A statement that the details for each specific coupon distribution program must be submitted under separate cover to the IGB Administrator for approval prior to implementation and must include the following information:

    a. The aggregate dollar value of promotional coupons, which include match play coupons, cash, chips or electronic credits authorized;
    b. The start and expiration dates of the program;
    c. Details regarding the issuance and controls over the issuance of coupons;
    d. Name of the direct mail house or outbound electronic mailing vendor or an indication that coupons will be printed in-house; and
    e. A sample of the coupon or outbound electronic coupon mailing.

2. A statement that the IGB Administrator and the IGB Docksite Supervisor must be notified in writing when any approved coupon program is discontinued prior to the expiration date.

3. Procedures for ensuring the coupon mailing/distribution list does not include any person on the IGB statewide voluntary self-exclusion list, the Owner Licensee's property based self-exclusion list and the IGB's Board exclusion list.

4. A statement that coupons may not be redeemed by mail.

5. A statement that the IGB Docksite Supervisor/Agent must be notified immediately of an incident where a coupon is presented for redemption which the system indicates has already been redeemed or there is a coupon which is suspected to be counterfeit, tampered with or altered in any way.

6. A statement of who is responsible for the review of the internal controls and security measures employed by the direct mail house or outbound electronic mailing vendor.

Past-Due Support Program

1. Owner Licensees must comply with the provisions of 89 Ill. Admin. Code 160.70 q).

2. Owner Licensees are required to include procedures for the collection and remittance of intercepted past-due support owed by responsible relatives from winnings required to be reported to the Internal Revenue Service on Form W2-G to the Illinois Division of Child Support Services. This process will be accomplished via the Department of Healthcare and Family Service's *Gaming Intercept Program Certification System* (GIPCS) website. The ICS must address the following:

    a. Procedures for the administration of authorized users, including:

i. user accounts and passwords must be issued and controlled by a System Administrator or their equivalent as listed in the ICS;
ii. updating or changing of user information (passwords, names, terminations, etc.);

b. Procedures for individuals authorized to provide the responsible relative with a receipt of the withheld winnings;
c. Procedures for individuals authorized to remit payment, net of the administrative fee, from the GIPCS to the Illinois Division of Child Support Services; and
d. Procedures for when authorized employees are unable to access the GIPCS website.

3. The ICS must include procedures for immediately notifying Security, Surveillance, and an IGB Docksite Supervisor/Agent when a person is confirmed in the Past Due Support Program.

Wireless Networks

1. For purposes of this section the following words and terms will have the following meanings:

"Critical Gaming Systems and equipment" includes all components of systems hardware and software, application software (e.g., slot accounting systems, bonusing systems, promotional systems, cashless wagering systems, player tracking system), and database software that individually or in combination are used for gaming operations.

"Vulnerability" is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be accidentally triggered or intentionally exploited and result in a security breach or a violation of the system security policy.

2. An Owner Licensee may use casino owned or leased wireless devices to communicate with the critical gaming system(s). A list of locations and boundaries of the wireless network must be submitted to the IGB Administrator or designee for approval. The use of wireless devices with the critical gaming system(s) does not replace any controls currently in place pertaining to the existing critical gaming system(s), as outlined in the MIS section of the Owner Licensee Internal Control System.

3. The Owner License must submit to the IGB Administrator or designee a topology diagram showing how the critical gaming system(s) interact, including a description of the purpose of the wireless devices/networks, a description of the system(s) accessible through wireless devices/networks and the job titles of those employees authorized to administer the wireless network access to wireless devices/networks.

4. Wireless networks used in conjunction with the critical gaming system(s) and equipment must meet the following minimum standards:

a. Wireless networks must implement authentication and encryption to ensure all wireless devices are authorized to be on the wireless network and all data packets transmitted on the wireless network are encrypted before being transmitted. Wireless network components must use and implement cryptographic modules

and algorithms which comply with the Federal Information Protection Standard 140-2, et seq. (FIPS 140-2), unless otherwise approved in writing by the IGB Administrator. The Owner Licensee or Licensed Supplier must maintain all FIPS certificates;

b. Wireless client operating systems must be hardened to provide adequate security in accordance with guidelines released by the NIST's Computer Security Resource Center (CSRC) that most appropriately fit the Owner Licensee's environment. For operating systems that are not addressed in the NIST CSRC guidelines, the Owner Licensee may instead harden wireless client operating systems in accordance with Security Technical Implementation Guides (STIGs) released by the Defense Information Systems Agency (DISA);

c. Communications between the server(s) and the wireless device must use appropriate authentication methods that utilizes current FIPS compliant cryptographic protocols for security to provide for validated authentication of the wireless device and the server in order to ensure the integrity and security of the data being transmitted. The wireless network, at a minimum, must utilize the IEEE 802.11i standard with IEEE 802.1x authentication. No communication can take place prior to successful authentication between the supplicant and the authentication server. Owner Licensees must immediately notify the IGB Administrator and the IGB Docksite Supervisor about vulnerabilities that become known to the licensee along with the expected time line to remedy;

d. The wireless deployment must employ a secure gateway (e.g. firewall) to isolate the wireless environment from any other environment (e.g. internal network). The secure gateway must be configured in a manner that prevents any wireless network component from gaining access to the internal network without first being scrutinized. For each allowance defined within the secure gateway's access control (i.e., policy) the following must be documented:

1) Business requirement;
2) Source IP address, protocol, and port; and
3) Destination IP address, protocol, and port;

e. All aspects pertaining to the installation of a wireless device/network, including all hardware and software utilized therein, must be subject to testing by an independent testing laboratory as prescribed by the IGB; and

f. If any authentication credentials are hard coded on a component of the wireless network, they must be encrypted.

5. Written approval must be obtained from the IGB Administrator prior to:

a. Connecting any wireless network components (routers, appliances, access points) to the gaming wireless network infrastructure. Replacement network components

must be restored to the IGB approved wireless configuration before connecting to the wireless system. Owner Licensees must submit a list of the type and number of individual network components added along with the corresponding MAC address. In addition to approval by the IGB Administrator, the IGB Docksite Supervisor must be notified in writing whenever a component is disconnected.

6. Written notification must be provided to the IGB Docksite Supervisor/Agent when changing or modifying the configuration of any gaming accessible wireless network component.