CHOCTAW NATION OF OKLAHOMA

CHOCTAW NATION GAMING COMMISSION

TECHNICAL STANDARDS AND PROCEDURES
FOR ELECTRONIC GAMING
UNDER THE
TRIBAL-OKLAHOMA STATE COMPACT AND 25 CFR PART 547

ISSUED BY THE CHOCTAW NATION OF OKLAHOMA GAMING COMMISSION
on February 17, 2023

Table of Contents

CHAPTER 1

POLICY AND GENERAL DEFINITIONS

1.1 INTRODUCTION

The Choctaw Nation Gaming Commission (CNGC) sets forth these Electronic Game Standards to govern the operation of both Class II and Compact gaming systems. At a minimum, the Class II Gaming Systems are required to meet 25 CFR Part 547, October 22, 2012, Minimum Technical Standards for Class II Gaming Systems and Equipment. Class II Gaming Systems are also required to meet the requirements set forth herein where the requirements are not in conflict of the Class II Technical Standards. In the event that there is a conflict, the Class II Technical Standards and applicable sections of the Tribal Internal Control Standards (TICS) shall supersede. Compact gaming systems are required to meet the requirements set forth in the Compact.

1.2 GENERAL STATEMENT

These Uniform Technical Standards and Procedures ("Uniform Standards") have been promulgated by the CNGC, the governmental gaming regulatory agency of the Choctaw Nation of Oklahoma ("Tribe"), to implement the requirements for operating electronic gaming under the Tribal-State gaming compact entered into between the Tribe and the State of Oklahoma in January, 2005, pursuant to Oklahoma Senate Bill 1252 ("Compact") and 25 CFR Part 547 Minimum Technical Standards for Class II Gaming Systems and Equipment. Electronic gaming under the Compact consists of three kinds of games: an "Electronic Amusement Game," an "Electronic Bonanza-Style Bingo Game," and an "Electronic Instant Bingo Game." 25 CFR Part 547 defines the technical requirements for Class II games. Electronic gaming may not be engaged in a Choctaw Nation of Oklahoma gaming facility unless the equipment used to play the game has been certified by an independent testing laboratory ("ITL") and the CNGC as conforming to these Uniform Standards. The process for seeking such certification is set forth herein.

1.3 DEFINITIONS

As used in these Uniform Standards, the following terms shall have the following meanings:

1) "Compact" means the Tribal-State gaming compact entered into between the Tribe and the State of Oklahoma in January 2005, pursuant to Oklahoma Senate Bill 1252.

2) "Electronic Amusement Game" means a game that is played in an electronic environment in which a patron's performance and opportunity for success can be improved by skill that conforms to the standards set forth in the State-Tribal Gaming Act.

3) "Electronic Bonanza-Style Bingo Game" means a game played in an electronic environment in which some or all of the numbers or symbols are drawn or electronically determined before the electronic bingo cards for that game are sold that conforms with the standards set forth in the State-Tribal Gaming Act.

4) "Electronic Instant Bingo Game" means a game played in an electronic environment in which a

patron wins if his or her electronic instant bingo card contains a combination of numbers or symbols that was designated in advance of the game as a winning combination. There may be multiple winning combinations in each game and multiple winning cards that conform to the standards set forth in the State-Tribal Gaming Act.

5) "Class II Games" means the game of chance commonly known as bingo, whether or not electronic, computer, or other technologic aids are used in connection therewith, including, if played in the same location, pull-tabs, lotto, punch boards, tip jars, instant bingo, and other games similar to bingo, as well as various non-house banked card games.

6) "Independent Testing Laboratory" or "ITL" means a laboratory of national reputation that is demonstrably competent and qualified to scientifically test and evaluate devices for compliance with the Compact and these Uniform Standards, and to otherwise perform the functions assigned to it. An ITL shall not be owned or controlled by the tribe, the enterprise, an organizational licensee as defined in the State-Tribal Gaming Act, the State, or any manufacturer, supplier or operator of gaming devices.

7) "Player Interface" means electronic or electromechanical Interfaces housed in cabinets with input devices and video screens or electromechanical displays on which patrons play Electronic Bonanza-Style Bingo Games, Electronic Instant Bingo Games or Electronic Amusement Games and Class II games.

8) "Uniform Standards" means these Uniform Technical Standards and Procedures.

CHAPTER 2

AUTHORIZED ELECTRONIC GAMES

2.1 INTRODUCTION

2.1.1 GENERAL STATEMENT.

The following electronic games are authorized pursuant to the Compact and 25 CFR Part 547. All equipment on which such games are to be played at any Choctaw Nation of Oklahoma gaming facility shall satisfy the requirements of these Uniform Standards. No games failing to meet the requirements of the Compact may be played on Player Interfaces. The following electronic games are permitted at Choctaw Nation of Oklahoma gaming facilities, and are further described in the sections that follow:

a) Electronic Amusement Games;

b) Electronic Bonanza-Style Bingo Games;

c) Electronic Instant Bingo Games.

d) Class II Games

2.2 ELECTRONIC AMUSEMENT GAMES

2.2.1 GENERAL STATEMENT.

Electronic Amusement Games must meet the following specifications:

a) Electronic Amusement Games shall be played through the employment of Player Interfaces which, following the payment of a fee, present games in which the patron can win prizes in a format in which a patron's performance can be improved by skill.

b) Available Games and Game Rules. The available games must be displayed on the Player Interface's video screen or otherwise prominently displayed on the Interface. The rules of the game must also be displayed either prominently on the Interface or on a help screen, and include sufficient information to alert novice patrons on the concept of the game so that a novice patron can understand how to improve his or her performance. Depending on the game selected, the patron must physically interact with the screen (through touch screen technology) or by depressing or activating buttons or other input devices, to cause an intended result.

c) Payment to Begin Play. A patron purchases an opportunity to play an Electronic Amusement Game at a Player Interface either through the insertion of currency, a voucher or ticket (i.e., cash or non-cashable, promotional voucher/ticket/credit), through the use of a cashless transaction system, or through credits on the credit meter.

d) Accountability Following Play. Following every play on a Player Interface, data shall be

maintained electronically and shall be viewable either electronically and/or by printed report. Such data shall provide basic information regarding the amount paid in, the game played, the result, and the prize awarded, if any. Such recording shall be monitored and regulated to ensure full accountability and integrity of play.

e) Payment Following Play. Following play on a Player Interface, the result shall be displayed and prizes awarded. Prizes may be dispensed in the form of currency, voucher or ticket, credits placed on the Player Interface's credit meter, merchandise or through a cashless transaction system.

f) Auditability of Software. For auditing, regulatory and security purposes, any Electronic Amusement Game shall include and have available a secure software tool to audit the software of each Electronic Amusement Game. Such tool shall be used only during authorized audits of Electronic Amusement Games, or in cases of patron disputes.

2.2.2 ELECTRONIC AMUSEMENT GAME SPECIFICATIONS.

Electronic Amusement Games are games in which a patron's performance can be improved by skill. Each Player Interface employed in an Electronic Amusement Game shall only offer games that meet the following minimum standards:

a) Each Electronic Amusement Game must require decisions or actions by patrons that could affect the result of the game;

b) No auto-hold, "smart-hold," or similar feature shall be employed which permits the Player Interface to automatically determine optimum play or make decisions for patrons;

c) Each Player Interface must prominently display either on the Interface or on a help screen:

   i) The rules of the game and instructions and other information regarding the concept of the game so that a novice patron can understand how to improve his or her performance; and

   ii) Possible winning combinations based on the amounts paid to play the game and the other information required in this section. Such information may not be incomplete, confusing or misleading.

d) In Electronic Amusement Games in which patrons are competing against others, the patrons shall be informed about whether and how winning prizes will be shared; and

e) No Electronic Amusement Game shall base its outcome on the number or ratio of prior wins to prior losses or any other factor relating to the profit or revenues retained by the operator from prior plays of the game.

2.3 ELECTRONIC BONANZA-STYLE BINGO GAMES

2.3.1 GENERAL STATEMENT.

Electronic Bonanza-Style Bingo Games must meet the following specifications:

a) Electronic Bonanza-Style Bingo Games shall only be conducted using a system that uses linked Player Interfaces that allow patrons to purchase and play electronic bonanza-style bingo cards. Patrons compete, following the payment of a fee, to be the first patron to cover a previously designated bingo pattern using a set of numbers or symbols at least some of which were drawn or electronically determined before the sale of bingo cards began. The first patron to cover the game-winning pattern wins the game-winning prize. Interim and consolation prizes also may be awarded.

b) Available Games and Game Rules. The available games must be displayed on the Player Interface's video screen or otherwise prominently displayed on the Interface. Depending on the game selected, the patron must physically interact with the screen (through touch screen technology) or by depressing or activating buttons or other input devices, to cause an intended result.

c) Payment to Begin Play. A patron purchases an opportunity to play an Electronic Bonanza-Style Bingo Game at a Player Interface either through the insertion of currency, a voucher or ticket (i.e., cash or non-cashable, promotional voucher/ticket/credit), through the use of a cashless transaction system, or through credits on the credit meter.

d) Accountability Following Play. Following every play on a Player Interface, data shall be maintained electronically and shall be viewable either electronically and/or by printed report. Such data shall provide basic information regarding the amount paid in, the game played, the result, and the prize awarded, if any. Such recording shall be monitored and regulated to ensure full accountability and integrity of play.

e) Payment Following Play. Following play on a Player Interface, the result shall be displayed and prizes awarded. Prizes may be dispensed in the form of currency, voucher or ticket, credits placed on the Player Interface's credit meter, merchandise or through a cashless transaction system.

f) Auditability of Software. For auditing, regulatory and security purposes, any Electronic Bonanza-Style Bingo Game shall include and have available a secure software tool to audit the software of each Electronic Bonanza-Style Bingo Game. Such tool shall be used only during authorized audits of Electronic Bonanza-Style Bingo Game, or in cases of patron disputes.

g) Numbers or Symbols. After the patron purchases a bingo card, the Player Interface must cover any numbers or symbols on the patron's bingo card that match numbers or symbols at least some of which were previously drawn or electronically determine for that game.

h) Display of Game Results. Although the results of the bingo game may be shown using entertaining video and/or mechanical displays, the patron may have the option to view the electronic bingo card and current ball draw on the video screen of the Player Interface.

2.3.2 ELECTRONIC BONANZA-STYLE BINGO GAME SPECIFICATIONS.

The following are general rules that govern the conduct of Electronic Bonanza-Style Bingo Games using Player Interfaces:

a) Electronic Player Interfaces must be designed to comply with the standards defined in the Compact, where applicable.

b) For purposes of this standard, a game server and an accounting server may be housed in the same physical device. This device must be separate from the Player Interfaces and must be kept in a secured location within the gaming venue.

2.3.3 General Player Interface Requirements.

For Player Interfaces connected to a game server, the following standards shall apply:

a) The game server shall generate and transmit to the bank of Player Interfaces a set of random numbers, colors and/or symbols, some of which are drawn prior to the sale of bingo cards. The subsequent game results are determined at the Player Interface and the resulting information is transmitted to the account server;

b) The game servers shall be housed in a game server room or secure locked cabinet outside of the Player Interface;

c) The following are the Electronic Bonanza-Style Bingo Game Server requirements for ball drawing:

   i) The balls shall be drawn via an approved electronic RNG certified for use in the game of Bingo or be drawn by an approved Mechanical RNG (such as a ball blower);

   ii) The operator shall have no discretion over which balls are drawn; and

   iii) The Game Server shall have the ability to pre-draw and transmit the drawn balls to the individual Player Interfaces prior to the sale of cards for that game, provided that it is understood that not all balls need to be pre-drawn.

2.4 Electronic Instant Bingo Games

2.4.1 General Statement.

Electronic Instant Bingo Games must meet the following specifications:

a) Patrons receive, after the payment of a fee, an electronic instant bingo card. A patron wins if his or her card contains a combination of symbols or numbers which was designated in advance of the game as a winning combination. There may be multiple winning combinations in each game and multiple winning cards. Electronic Instant Bingo Games shall only utilize Player Interfaces which allow patrons to purchase and play electronic instant bingo cards. Consistent with this intent, each Player Interface employed in an Electronic Instant Bingo Game shall meet the following minimum standards:[1]

b) Available Games and Game Rules. The available games must be displayed on the Player Interface's video screen or otherwise prominently displayed on the Interface. Depending on the

[1] It should be noted that the Act is unclear as to whether Electronic Instant Bingo Games can be played on the same Interfaces that offer Electronic Bonanza-Style Bingo Games or Electronic Amusement Games, however, taking the document as a whole, this appears to be allowed.

game selected, the patron must physically interact with the screen (through touch screen technology) or by depressing or activating buttons or other input devices, to cause an intended result.

c) Payment to Begin Play. A patron purchases an opportunity to play an Electronic Instant Bingo Game at a Player Interface either through the insertion of currency, a voucher or ticket (i.e., cash or non-cashable, promotional voucher/ticket/credit), through the use of a cashless transaction system, or through credits on the credit meter.

d) Accountability Following Play. Following every play on a Player Interface, data shall be maintained electronically and shall be viewable either electronically and/or by printed report. Such data shall provide basic information regarding the amount paid in, the game played, the result, and the prize awarded, if any. Such recording shall be monitored and regulated to ensure full accountability and integrity of play.

e) Payment Following Play. Following play on a Player Interface, the result shall be displayed and prizes awarded. Prizes may be dispensed in the form of currency, voucher or ticket, credits placed on the Player Interface's credit meter, merchandise or through a cashless transaction system.

f) Auditability of Software. For auditing, regulatory and security purposes, any Electronic Instant Bingo Game shall include and have available a secure software tool to audit the software of each Electronic Instant Bingo Game. Such tool shall be used only during authorized audits of Electronic Instant Bingo Game, or in cases of patron disputes.

g) Numbers or Symbols. After the patron purchases a bingo card, the Player Interface must cover any numbers or symbols on the patron's bingo card that match numbers or symbols at least some of which were previously drawn or electronically determine for that game.

h) Display of Game Results. Although the results of the bingo game may be shown using entertaining video and/or mechanical displays, the patron may have the option to view the electronic bingo card and current ball draw on the video screen of the Player Interface.

2.4.2 ELECTRONIC INSTANT BINGO GAME SPECIFICATIONS.

The following are general rules that govern the conduct of Electronic Instant Bingo Games using Player Interfaces:

a) Electronic Instant Bingo Game Interfaces must be designed to comply with the standards defined above, where applicable and not modified by this section.

b) Electronic Instant Bingo Game Interfaces, to be distinguished from "slot machines" (the latter not being allowed) must operate in a manner in that the card in which the patron purchases already has a game outcome on it and the purchase of which allows for payment. Therefore, it appears to be assumed that a patron must purchase an opportunity or game outcome from a predetermined set of game outcomes or electronic instant bingo cards.

c) Such predetermined set, noted in (b) above, would need to be a finite pool of predefined sets of

outcomes, but need not be a pool of outcomes that are dispensed "without replacement."

d) The dispensing of the predetermined outcome must be performed randomly.[2]

[2] Instant bingo cards are game outcomes that must be created prior to game play. Tickets must be finite in number, but may be replaced or not at the end of each game play (allow either replacement or not replacement.)

CHAPTER 3

TESTING AND CERTIFICATION PROCEDURES AND REQUIREMENTS

3.1 CERTIFICATION SUBMISSION PROCESS AND REQUIREMENTS

3.1.1 INDEPENDENT TESTING LABORATORY ("ITL").

The CNGC shall maintain a list of approved ITLs.

3.1.2 SUBMISSION PROCESS.

Submissions to an ITL may be made at any time by a manufacturer, distributor or vendor of electronic equipment proposed to be used for playing electronic games authorized by the Compact and or 25 CFR Part 547 at a Choctaw Nation of Oklahoma facility, provided that the certification sought shall be for conformity with these Uniform Standards or with any comparable technical standards and procedures the CNGC deems appropriate. A list of comparable standards and procedures may be obtained upon request from the CNGC. The CNGC reserves the right to withdraw its approval at any time of the use of standards and procedures other than these Uniform Standards.

3.1.3 PREVIOUS SUBMISSIONS.

Where on a previous submission, the ITL has been provided with the data necessary to test the electronic equipment in question to these Uniform Standards, verification of that fact from the ITL may be relied upon to avoid duplicate submission of data. Every effort shall be made to reduce the redundancy of submission information.

3.1.4 PROTOTYPE SUBMISSION (FULL SUBMISSION).

A Prototype Submission is a first-time submission of a particular piece of hardware or software that has not previously been reviewed by an ITL. The following items shall be provided with each prototype's initial submission:

a) Submission Letter. Each submission shall include a request letter, on company letterhead, dated within one (1) week of the date the submission is received by the ITL. The letter shall include the following:

   i) The jurisdiction(s) for which certification is requested;

   ii) The items requested for certification. In the case of software, the submitting party shall include ID numbers and revision levels, if applicable. In the case of hardware, the submitting party shall indicate the manufacturer, supplier, and model number of the associated components of hardware; and

   iii) A contact person who will serve as the main point of contact for engineering questions raised during evaluation of the submission. This may be either the person who signed the letter or another specified contact.

b) When a Random Number Generator (RNG) Submission is needed. In some cases, the RNG shall be submitted with the Prototype Submission request (for specific RNG Submission details, refer to Section 3.1.5, of this document). RNGs shall be submitted for certification where:

   i) The RNG code has changed from a previously certified RNG or the implementation of the random number has changed; or

   ii) Where a previously certified RNG is being implemented on a new hardware platform (i.e., change of microprocessor); or

   iii) Where a previously certified RNG is generating numbers that are outside the range of numbers previously tested; or

   iv) The RNG has never been certified before under these Uniform Standards. In this case, the RNG will be certified as a part of the overall submission.

c) All accompanying technical documents, manuals and schematics shall be submitted. In addition, the following items shall be provided:

   i) If applicable, all UL, CSA, EC, AS3100, etc., or equivalent certification;

   ii) Any other equipment that may be used in the field in conjunction with the submission;

   iii) Accompanying software;

   iv) If the submitting party has specialized equipment that is needed by the ITL to test the submitted device, then the specialized equipment and all appropriate operation manuals for the equipment shall be included with the submission; and

   v) If requested, extension cables for door photo-optic detectors and any other hardware should be provided, so that the Player Interface may be tested with doors opened. In addition, where a processor board is oriented in a Player Interface in such a way that it would be difficult to install a plug and cable from an emulator, extension cables should be provided to allow the board to be relocated. The use of such extension cables shall not adversely affect the machine's operation.

d) Two sets of all EPROMs, CD-ROMs, or other storage media, which contain identical contents. This includes all video, sound, printer, touch screen, bill acceptor, protocol clear, and game software. On the program medium that is submitted, where applicable, and subsequently placed in the field, each program shall be uniquely identified, displaying the program ID number, manufacturer, version number, type and size of medium (unless located on the medium as purchased unused from the supplier), and location of installation in Player Interface, if potentially confusing. For EPROM-based games, the identification label shall be placed over the UV window to avoid erasing or alterations of the program.

e) Percentage Calculation Sheets. For each game submitted, the manufacturer shall supply the

calculation sheets that determine the theoretical return to the patron including the base game, double-up options, free games, bonus features, etc. (This would also include where different patron options (e.g., number of credits bet) vary the pay table. A separate calculation for each option or patron strategy is required. Where a game requires or allows use of patron strategy that can affect the outcome of the game, along with the continuing actual patron return, the manufacturer shall list the assumed patron strategy used in the theoretical calculations of the patron return and the source of said strategy. For games with patron strategy, if available, actual game return statistics from development laboratories or field trials of the game in other jurisdictions shall be submitted. If the manufacturer fails to provide this information, the ITL will calculate the outcome prior to approval.)

f) A written Statement of Verification that a previously certified RNG is used within the submitted software.

g) A legible, color copy of the payglass (if applicable).

h) Source Code, a Link Map and Symbol Table. In addition, if requested, explanation of all non-volatile RAM on the device with the non-volatile RAM locations described. (All Source Code submitted shall be correct, complete and able to be compiled. The result of the compiled object code shall be identical to that in the storage medium submitted for evaluation. All Source Code submitted should be commented in an informative and useful manner.) Further, the submitting person or entity must comply with all of the ITL's requests for additional Source Code information.

i) A manual explaining all diagnostic tests, meters, game configurations, error conditions and how to clear them.

j) RAM clear procedures.

k) A general overview of the system, describing how the software and hardware are integrated.

l) Program block diagrams and flow charts for the game program.

m) For all software involved in control of gaming functions, provide an assembler, linker, formatter, or other computing utilities as is necessary to generate the installed gaming software from the Source Code supplied. This requirement may be waived where program code is written in assembler and the listing file (showing the assembled and link code) is provided. If a non-PC-based platform development system is used, the manufacturer shall supply the ITL with the necessary computer equipment and software necessary to compile and verify the final executable program.

Permission to exclude any of the above requirements may be granted upon written request to the CNGC.

3.1.5 RNG SUBMISSIONS.

An ITL may use PC-based RNG gathering programs to collect data from Player Interfaces or other medium through a communications port. Adherence to the specifications below allows the submitting party to use the ITL's PC-based RNG gathering program, where applicable. Use of this protocol is not required; however, in that case, the submitting party shall supply the software collection interface software for the ITL's use, which will be reviewed prior to implementation. The following describes the implementation of the ITL's remote protocol unless otherwise specified by the ITL:

a) The manufacturer shall supply correct settings to interface to their machine; the object of such test is that random numbers, as the patron would receive them, is reviewed:

   i) In electronic Poker, the ten (10) cards following the shuffle (it is recommended, but not required, to send the first five (5) cards dealt; then the five (5) draw cards);

   ii) In electronic Blackjack, the top eighteen (18) cards following the shuffle;

   iii) For skill-style spinning reel devices, the Player Interface shall provide three (3) stops/symbols for a 3-reel game, five (5) stops/symbols for a 5-reel game, etc. The game should return the virtual stops/symbols selected for each reel;

   iv) For bingo games, the seventy-five (75) numbers as they are drawn;

   v) For instant bingo games, those numbers or symbols that make up the winning combination or the game outcome designation;

   vi) For any other type of game or bonus game, please contact the ITL for guidance; and

   vii) The test program RNG shall be identical to the RNG contained in the game software except for the following changes, which may be implemented to speed up the requirements of the test. The ITL may not allow any of the following changes where it determines such change might affect the data received from the RNG. It should be noted that production software may have a test mode that contains this imbedded RNG test mode, provided that the Player Interface indicates clearly that it is in said test mode.

   viii) RNG submission requirements for Class II games are defined within 25 CFR Part 547 Technical Standards.

b) The RNG test program should not require credits on the Player Interface in order to play.

c) The RNG test program should not award credits and not lock up for award pays.

d) The RNG test program does not have to show the game play. The program can just display a message that states RNG test in progress.

e) The manufacturer shall supply the ITL with detailed instructions on how to set-up the Player Interface for test.

f) The manufacturer shall supply the ITL with a detailed description of the RNG Algorithm that includes a detailed description on the RNG implementation in their device, including how the initial SEED is generated. In addition, it shall provide the Algorithm for reseeding or changing of the seed during game play, if applicable.

g) The manufacturer shall submit a cable to connect from the Player Interface to a PC-based computer. This cable will utilize serial-type communications and easily attach to a standard PC. If any special

attachments or converters are necessary, the submitting party shall supply the equipment.

h) The ITL may employ the use of various approved tests to determine whether or not the random values produced by the RNG pass the desired confidence level of 99%. CNGC shall maintain a list of approved tests.

i) Mechanical-based RNG games must meet the following requirements:

    i) The ITL will test via PC communications multiple iterations to gather enough data to verify the randomness. In addition, the manufacturer may supply live data to assist in this evaluation;

    ii) The mechanical components that have an impact on the determination of the random outcome must not deteriorate over time;

    iii) The properties of physical items used to choose the selection shall not be altered; and

    iv) The patron shall not have the ability to physically interact or come into physical contact or manipulate the Player Interface physically with the mechanical portion of the game.

3.1.6 Submitting Modifications to a Previously Certified Item.

For any update submission, the following information shall be required to process the submission in addition to the requirements set forth in Section 3.1.4 for the submission letter. This process is intended to speed up the administrative burden of modification submissions. All modifications require re-testing, examination and re-certification by an ITL approved by the CNGC.

a) Each hardware submission shall:

    i) Identify the individual items being submitted (including part number);

    ii) Supply a complete set of schematics, diagrams, data sheets, etc., describing the modification along with the reason for the change(s); and

    iii) Provide the updated or new device, a description and the method of connection to the original Player Interface or hardware.

b) Each software submission shall:

    i) Use the same requirements as in Section 3.1.4, Prototype Submission, except where the documentation has not changed. In this case, a resubmission of identical documentation is not required. (Such as if the paytable and mathematics of the game are not changed, the submitting party may refer to previous documentation); and

    ii) Include a description of the software change(s), modules affected and new Source Code for the entire program. Source code is required for the entire program to check compile and Source Code integrity.

3.1.7 JOINT VENTURE SUBMISSIONS.

A Player Interface is considered a joint venture when two or more companies are involved in the manufacturing of one platform. In an effort to alleviate confusion among the suppliers, the regulator, and the ITL, the following procedures must be met for such submissions:

a) One company will prepare and submit the entire submission, even if they are using parts from other suppliers, and must identify the part numbers of all components. This company will be the primary contact for the submission.

b) The company submitting an approval request should do so on their letterhead.

c) The ITL will delegate an internal file number in this company's name and will bill this company for all costs incurred throughout the approval process.

d) The primary contact will be called when questions arise. However, test engineers will work with all parties involved in order to complete the review.

e) All parties who are part of the submission group may need to be licensed in the jurisdiction(s) where the submission is being approved. As a courtesy to the supplier, the ITL may inquire as to whom does not need to be licensed from the regulator client. It should be noted that licensing questions should be handled directly with the CNGC.

f) Upon completion, it is the primary contact company that will receive the approval letter, provided the submission meets the jurisdictional requirements. The primary contact company may then release copies of the approval letter to the associated manufacturer(s).

CHAPTER 4

TRIBAL APPROVAL AND CERTIFICATION

4.1 APPLICATION TO TRIBAL GAMING COMMISSION

Once certification is obtained from the ITL that the equipment in question meets all applicable regulations set forth herein for that type of equipment and the game or games to be played thereon or therewith, an application for Tribal certification may be sought from the CNGC. All applications for approval shall be on the forms prescribed by the CNGC and accompanied by all processing fees required by that agency and proof that a Tribal gaming license has been issued or an application has been properly filed with the CNGC. No application for certification shall be considered by the CNGC unless and until the required processing fees have been paid along with proof of the Tribal gaming license or that a proper application for a license is pending in good standing. All certification applications shall be reviewed for compliance with the regulations herein and certification by the ITL that its process has been satisfactorily completed and that the equipment meets these regulations. The CNGC may, but is not required to, accept issuance of a certificate of compliance with these or comparable regulations by another Tribe subject to a compact similar to the Compact herein.

4.2 TIME FOR ISSUANCE

The CNGC shall make reasonable efforts to complete its review processes within 60 days of submission, but the timing and requirements for approval shall be subject to the sole discretion of the CNGC.

4.3 CERTIFICATE OF COMPLIANCE

Upon approval of the submission application, the vendor may, subject to obtaining all necessary gaming licenses from the CNGC, offer the game to the Tribe for use in a Choctaw Nation of Oklahoma gaming facility. Certificates of compliance shall be valid for two years and shall be renewed on terms set forth by the CNGC.

CHAPTER 5

PLAYER INTERFACE AND USE REQUIREMENTS FOR AUTHORIZED GAMES

5.1 COMPACT REQUIREMENTS

5.1.1 GENERAL PLAYER INTERFACE REQUIREMENTS.

Player Interfaces used in connection with electronic games shall conform to the following standards:

a) All Player Interfaces shall be capable of being used with an Online Accounting System (OAS).

b) In addition to a video monitor or other electromechanical display, each Player Interface may have one or more of the following: a printer, graphics, and/or signage.

c) Each Player Interface may have one or more of the following: electronic buttons, touch screen capability, and/or a mechanical, electromechanical or electronic means of activating the game and providing patron input, including a means for making patron selections and choices in games.

d) Each Player Interface shall have a nonvolatile backup memory or its equivalent, which shall be maintained in a secure compartment on each Player Interface for the purpose of storing and preserving a redundant set of critical data which has been error checked in accordance with the Compact, and which data shall include, at a minimum, the following Player Interface information:

    i) Electronic meters as required by the Technical requirements set forth in Section 5.2.37 of these Uniform Standards.

    ii) Recall of all wagers and other information associated with the last ten (10) plays; and

    iii) Error conditions that may have occurred on the Player Interface.

e) Each Player Interface shall have an on/off switch that controls the electrical current that supplies power to the Player Interface, which must be located in a secure place that is readily accessible within the interior of the Player Interface.

f) The operation of each Player Interface must not be adversely compromised or affected by static discharge, liquid spills, or electromagnetic interference.

g) Each Player Interface must have electronic accounting meters which have tally totals to a minimum of seven (7) digits and be capable of rolling over when the maximum value of at least 9,999,999 is reached. The Player Interface must provide a means for on-demand display of the electronic meters via a key switch or other secure method on the exterior of the machine. Electronic meters on each Player Interface for each of the following data categories are required:

    i) Credits, or equivalent monetary units, deposited on a cumulative basis on that Player Interface;

ii) If a Player Interface offers more than one style of game, as defined in Section 1.3 of these Uniform Standards, for play, then for each game, the meter shall record the number of credits, or equivalent monetary units, wagered and won for each game;

iii) hand-paid progressive and Mystery prizes paid for that Player Interface, which must include the cumulative amounts paid by an attendant for any such jackpot not otherwise metered pursuant to subparagraph (h) of this paragraph;

iv) The number of electronic games played on the Player Interface; and

v) The number of times the cabinet door is opened or accessed.

h) Under no circumstances shall the Player Interface electronic accounting meters be capable of being automatically reset or cleared, whether due to an error in any aspect of its or a game's operation or otherwise. All meter readings must be recorded and dated both before and after an electronic accounting meter is cleared.

i) At a minimum, each Player Interface shall have the following game information available for display on the video screen and/or displayed on the Player Interface itself, in a location conspicuous to the patron:

i) The rules of the game being played;

ii) The maximum and minimum cost of a wager, purchase or play activation and the amount of credits, or cash equivalents, which may be won for each game offered through that Player Interface;

iii) The patron's credit balance;

iv) The outcome of the game then being played; and

v) Any prize won on the game then being played.

j) The video screen or other means for displaying game rules, outcomes and other game information shall be kept under a glass or other transparent substance which places a barrier between the patron and the actual surface of the display. At no time may unauthorized stickers or other removable media be placed on the Player Interface's face (the front of the Interface, including its video screen) for purposes of displaying rules or payouts.

k) No hardware switches may be installed on a Player Interface or any associated equipment which may affect the outcome or payout of any game for which the Player Interface is used. Switches may be installed to control the ergonomics of the Player Interface.

l) Where the electronic game system or components are linked with one another in a local network for progressive and Mystery prizes, function sharing, aggregate prizes or other purposes, communication protocols must be used which ensure that erroneous data or signals will not

adversely affect the operations of any such system or components.

5.2 ADDITIONAL REQUIREMENTS

5.2.1 GENERAL STATEMENT.

This section reflects additional requirements that, while not specifically required by the Compact and 25 CFR Part 547, have been determined by the CNGC as being necessary to meet the Tribe's standards for electronic gaming. These requirements may also be required by the CNGC's internal control standards. All electronic games sought to be played in a Choctaw Nation of Oklahoma gaming facility pursuant to the Compact and 25 CFR Part 547 shall meet these additional requirements. It should be noted that all of these standards shall be met "where applicable" (e.g., if the device does not have a mechanical display, adherence to "mechanical display" requirements are not required).

5.2.2 PLAYER INTERFACE SECURITY.

The Player Interface must be able to withstand forced illegal entry, unless such entry causes an error code or is cleared at the commencement of a new play, and which does not affect the subsequent play or any other play, prize or aspect of the game.

5.2.3 PATRON SAFETY.

Electrical and mechanical parts and design principals of the Player Interface may not subject a patron to any physical hazards. The ITL shall not make any finding with regard to safety and electromagnetic compatibility (EMC) testing, as that is the responsibility of the manufacturer of the goods or those who purchase the goods.

5.2.4 MICROPROCESSOR CONTROLLED.

Each electronic game shall be controlled by one or more microprocessors or equivalent in such a manner that the game outcome is completely controlled by the microprocessor or a mechanical device (e.g., RNG). A microprocessor or mechanical device may be stored either locally on the electronic game or remotely on a server based product.

5.2.5 CABINET WIRING.

The Player Interface shall be designed so that power and data cables into and out of the Player Interface can be routed so that they are not accessible to the general public. This is for game integrity reasons only, not for health and safety. Security-related wires and cables that are routed into a logic area shall not be able to be easily accessed.

5.2.6 PLAYER INTERFACE IDENTIFICATION.

A Player Interface shall have a not easily removable (without leaving evidence of tampering) identification badge, permanently affixed to the exterior of the cabinet by the manufacturer, and this badge shall include the following information:

a) The manufacturer;

b) A unique serial number;

c) The Player Interface model number; and

d) The date of manufacture.

5.2.7 Player Interface Communications.

Player Interface Communications (PIC) shall provide a method of notification when: a patron has won an amount or is redeeming credits that the Player Interface cannot automatically pay, or an error condition has occurred or a "Call Attendant" condition has been initiated by the patron. A PIC may include, but is not limited to, a tower light, an audible alarm or a message displayed on the Player Interface.

5.2.8 Power Surges.

The Player Interface shall not be adversely affected, other than resets, by surges or dips of ± 20% of the supply voltage. Reset is acceptable only if no damage to the equipment or loss or corruption of data is experienced in the field.

5.2.9 External Doors/Compartments.

The following requirements shall apply to the Player Interface's external doors:

a) Doors shall be manufactured of materials that are suitable for allowing only legitimate access to the inside of the cabinet (that is, doors and their associated hinges shall be capable of withstanding determined illegal efforts to gain access to the inside of the Player Interface and shall leave evidence of tampering if an illegal entry is made);

b) All external doors which contain critical components shall be locked and monitored by door access sensors, which shall detect and report all external door openings, both to the Player Interface, by way of an error, and to an on-line system.

c) It shall not be possible to insert a device into the Player Interface that will disable a door open sensor when the machine's door is closed, without leaving evidence of tampering; and

d) The sensor system shall register a door as being open when the door is moved from its fully closed and locked position.

5.2.10 Logic Compartment.

The logic compartment is a locked cabinet area(s) with its own locked door, which houses critical electronic components that have the potential to significantly influence the operation of the Player Interface. There may be more than one such logic area in a Player Interface. Electronic component items that are required to be housed in one or more logic areas are:

a) CPUs and other electronic components involved in the operation and calculation or display of game

play (e.g., game controller electronics and components housing the game or system firmware program storage media); and

b) Communication controller electronics, and components housing the communication program storage media or, the communication board for the on-line system may reside outside the Player Interface.

5.2.11 CURRENCY COMPARTMENTS.

The currency compartments shall be locked separately from the main cabinet area. Currency compartments must also meet the following requirements:

a) Access to the currency storage area is to be secured via separate key locks and shall be fitted with sensors that indicate that the door has opened/closed or the bill stacker has been removed.

b) Access to the currency storage area is to be through two levels of locks, the relevant outer door plus one other door or lock, before the receptacle or currency can be removed.

5.2.12 FUNCTION OF A RANDOM ACCESS MEMORY (RAM) CLEAR.

Following the initiation of a RAM reset procedure (using a certified RAM clear method that is reviewed and evaluated by an ITL and approved by the CNGC), the game program shall execute a routine, which initializes each and every bit in RAM to the default state. For games that allow for partial RAM clears, the methodology in doing so must be accurate and the game must validate the un-cleared portions of RAM. The default reel position or game display after a RAM reset shall not be the top award on any selectable line. The default game display, upon entering game play mode, shall also not be the top award. This applies to the base game only and not any secondary bonus devices.

5.2.13 CONFIGURATION SETTING.

It shall not be possible to change a configuration setting that causes an obstruction to the electronic accounting meters without a RAM clear. Notwithstanding, any such change must be done by a secure means, which includes access to the locked logic area.

5.2.14 CRITICAL MEMORY DEFINED.

Critical memory storage shall be maintained by a methodology that enables errors to be identified and corrected in most circumstances. This methodology may involve signatures, checksums, partial checksums, multiple copies, timestamps and/or effective use of validity codes. Critical memory is used to store all data that is considered vital to the continued operation of the Player Interface. This includes, but is not limited to:

a) All electronic meters required in “electronic metering within the Player Interface,” including last bill data and power up and door open metering;

b) Current credits;

c) Player Interface/game configuration data;

d) Information pertaining to the last ten plays with the RNG outcome, including the current game, if incomplete; and

e) Software state (the last normal state the Player Interface software was in before interruption).

5.2.15 Critical Memory Integrity.

Comprehensive checks of critical memory shall be made during each Player Interface restart (such as power-up cycle). The Player Interface control program shall test for possible corruption of critical memory. Test methodology shall detect 99.99 percent of all possible failures. In addition, all critical memory (non-volatile) shall:

a) Have the ability to retain data for a minimum of thirty days after power is discontinued from the machine. If the method used is an "off chip" battery source, it shall re-charge itself to its full potential in a maximum of twenty-four hours. The shelf life of the battery source shall be at least five years. Random access memory that uses an off-chip back-up power source to retain its contents when the main power is switched off shall have a detection system which will provide a method for software to interpret and act upon a low battery condition;

b) Only be cleared by accessing the locked logic area in which it is housed;

c) Result in a RAM error if the control program detects an unrecoverable memory error; and

d) The RAM should not be cleared automatically, but shall require a full RAM clear (RAM Reset) performed by an authorized person.

5.2.16 Program Storage Devices.

All Program Storage Devices (writable/non-writable), including, but not limited to, EPROMs, DVD, CD-ROM, compact flash and any other type of Program Storage Devices, shall:

a) Be clearly marked with sufficient information to identify the software and revision level of the information stored in the devices and shall only be accessible with access to the locked logic compartment, where applicable; and

b) Be housed within a locked logic compartment.

5.2.17 Write Once (Non-Writable) Program Storage.

For Program Storage Devices that are written to once (i.e., EPROM, CD, compact flash, SIMM or DIMM flash module,), the following requirements shall be met:

a) CD-ROM specific based program storage shall:

    i) Not be a re-writeable disk; and

ii) The "session" shall be closed to prevent any further writing.

b) Non-EPROM specific (including CD-ROM) program storage shall meet the following requirements:

i) The control program shall authenticate all critical files by employing a hashing algorithm which produces a "message digest" output of at least 128 bits at minimum, as certified by the ITL. The message digest(s) shall be stored on a memory device (ROM-based or other medium) within the Player Interface. Message digests which reside on any other medium shall be encrypted, using a public/private key algorithm with a minimum of a 512 bit key. However, a 768 bit key is recommended, or an equivalent encryption algorithm with similar security certified by the ITL and approved by the CNGC.

ii) The Player Interface shall authenticate all critical files against the stored message digest(s), as required in Section 5.2.17(b)(i) above. In the event of a failed authentication, after the game has been powered up, the Player Interface should immediately enter an error condition with the appropriate PIC signal and record the details including time and date of the error in a log. This error shall require operator intervention to clear. The game shall display specific error information and shall not clear until either the file authenticates properly, following the operator intervention, or the medium is replaced or corrected, and the device's memory is cleared, the game is restarted, and all files authenticate correctly.

5.2.18 WRITABLE PROGRAM STORAGE.

This section applies to Player Interfaces where the control program is capable of being erased and re-programmed without being removed from the Player Interface. Bill acceptor or other equipment or related device shall meet the following requirements:

a) Re-programmable program storage shall only write to alterable storage media containing data, files, and programs that are not critical to the basic operation of the game. As an exception, such device may write to media containing critical data, files, and programs provided that such media:

i) Store a log of all information that is added, deleted, and modified;

ii) Shall be verified for the validity of all data, files, and programs which reside on the media using the methods listed in the Non-EPROM Specific requirements;

iii) Contain appropriate security to prevent unauthorized modifications;

iv) Does not allow game play while the media containing the critical data, files, and programs is in a modifiable state, unless otherwise approved by the Choctaw Nation Gaming Commission; and

v) For Client Server based Player Interface control program downloading, the rules outlined within Chapter 7 of this document shall also apply.

5.2.19 INTEGRITY OF THE CONTROL PROGRAM.

The control program shall ensure the integrity of all critical program components during the execution of said components and the first time the files are loaded for use (even if only partially loaded), where applicable. RAM and Program Storage Device (PSD) space that is not critical to machine security (e.g., video or sound ROM) are not required to be validated. If any of the video or sound files contain payout amounts or other information needed by the patron, the files or program storage must have a secure method of verification.

5.2.20 Multi Station Games.

A Multi-Station game is a gaming device that incorporates more than one Player Interface which may be controlled by a master Player Interface. The master Player Interface, containing the game's CPU, will house the game display, which is shared among the Player Interfaces. Each "station" must meet the technical standards outlined throughout this document, including Player Interface identification and metering. There must be a method for each patron to know when the next game will begin.

5.2.21 Printed Circuit Board Identification.

Requirements for printed circuit board identification include:

a) Each printed circuit board shall be identifiable by some sort of name (or number) and revision level;

b) The top assembly revision level of the printed circuit board shall be identifiable. If track cuts and/or patch wires are added to the printed circuit board, then a new revision number or level must be assigned to the assembly; and

c) Manufacturers shall ensure that circuit board assemblies, used in their Player Interfaces, conform functionally to the documentation and the certified versions of those printed circuit boards that were evaluated and certified by the ITL.

d) The CNGC shall be notified of any alteration to an ITL certified circuit board. The CNGC may require the manufacturer acquire recertification from an ITL approved by the CNGC following any alteration.

5.2.22 Mechanical Devices Used for Displaying Game Outcomes.

If a game has mechanical or electro-mechanical devices, which are used for displaying game outcomes, the following requirements shall be observed:

a) Electro-mechanically controlled display devices, such as reels or wheels, shall have a sufficiently closed loop of control so as to enable the software to detect a malfunction, or an attempt to interfere with the correct operation of that device. If a reel or wheel is not in the position it is supposed to be in, an error condition must be generated;

b) Where applicable, mechanical assemblies, such as reels or wheels, must have a mechanism that ensures the correct mounting of the assembly's artwork;

c) Displays shall be constructed in such a way that winning symbol combinations match up with pay lines or other indicators; and

d) A mechanical assembly shall be so designed that it is not obstructed by any other components.

e) Mechanical Reels for Class II games are utilized as 'Entertaining Displays' only and have no impact on the outcome of the game. However, the operation of the mechanical reels for Class II games shall adhere to the Class II Technical requirements.

5.2.23 VIDEO MONITORS/TOUCH SCREENS.

Touch screens must be accurate. Touch screens that require calibration, once calibrated, shall maintain that accuracy for at least the manufacturer's recommended maintenance period. Such touch screens must be able to be re-calibrated by venue staff without access to the Player Interface cabinet other than opening the main door. There shall be no hidden or undocumented buttons/touch points anywhere on a touch screen, except as provided for by the game rules that affect game play.

5.2.24 BILL ACCEPTORS.

All acceptance devices shall be able to detect the entry of valid bills, coupons, ticket vouchers, or other approved notes and provide a method to enable the Player Interface software to interpret and act appropriately upon a valid or invalid input. The acceptance device(s) shall be electronically-based and be configured to ensure that they only accept valid bills of legal tender. Bill acceptors may also accept coupons, ticket vouchers, or other approved notes and reject all others in a highly accurate manner. The bill input system shall be constructed in a manner that protects against vandalism, abuse, or fraudulent activity. In addition, bill acceptance device(s) shall only register credits when:

a) The financial instrument has passed the point where it is accepted and stacked; and

b) The acceptor has sent the "irrevocably stacked" message to the machine.

5.2.25 FINANCIAL INSTRUMENT COMMUNICATIONS.

All bill acceptors shall communicate to the Player Interface using a bi-directional protocol.

5.2.26 FACTORY SET BILL ACCEPTORS.

If bill acceptors are designed to be factory set only, it shall not be possible to access or conduct maintenance or adjustments to those bill acceptors in the field, other than:

a) The selection of bills, coupons, ticket vouchers, or other approved notes and their limits;

b) Changing of certified EPROMs or downloading of certified software;

c) Adjustment of the tolerance level for accepting bills or notes of varying quality should not be allowed externally to the machine. Adjustments of the tolerance level should only be allowed upon CNGC approval. This can be accomplished through lock and key, physical switch settings, or other accepted methods approved by the CNGC on a case-by-case basis;

d) Maintenance, adjustment, and repair per approved factory procedures; or

e) Options that set the direction or orientation of acceptance.

5.2.27 TOKENIZATION.

For games that allow tokenization, the game shall post for the patron the entire amount and not store fractional credits, unless the game maintains the credit meter in dollars and cents. If the game stores the credit meter in dollars and cents, then this rule would not apply.

5.2.28 ACCOUNTABILITY OF BILLS/TICKETS OR OTHER ITEMS ACCEPTED.

A Player Interface, which contains a bill acceptor device, shall maintain sufficient electronic metering to be able to report the following:

a) Total monetary value of all items accepted;

b) Total number of all items accepted; and

c) A breakdown of the bills accepted:

    i) For bills, the game shall report the number of bills accepted for each bill denomination;

    ii) For all other notes, the game shall have a separate meter that reports the number of notes accepted, not including bills.

5.2.29 BILL ACCEPTOR RECALL.

A Player Interface that uses a bill acceptor shall retain in its memory and display the denomination of the last five items accepted by the bill acceptor, including, for example, U.S. currency, ticket vouchers and coupons.

5.2.30 BILL ACCEPTOR ERROR CONDITIONS.

Each Player Interface and/or bill acceptor shall have the capability of detecting and displaying an error condition, for the conditions below. It is acceptable for the bill acceptor to disable or flash a light or lights to indicate the error has occurred, provided the information is communicated to the Player Interface and the bill acceptor disables:

a) Stacker full;

b) Bill jams;

c) Bill acceptor door open – where a bill acceptor door is the belly glass door, a door open signal is sufficient;

d) Bill stacker door open or bill stacker removed; and

e) Any error that impairs the functionality of the bill acceptor not specified above.

5.2.31 Bill Acceptor Stacker Requirements.

Each bill acceptor shall have a secure stacker and items accepted by the bill acceptor shall be deposited into the secure stacker. The secure stacker is to be attached to the Player Interface in such a manner so that it cannot be easily removed by physical force and shall meet the following requirements:

a) The bill acceptor device shall have a "stacker full" sensor;

b) There shall be a separate key to access the stacker compartment. This key shall be separate from the main door. In addition, a separate key shall be required to remove the bills from the stacker; and

c) A PIC shall be activated whenever there is access to the bill door or the stacker has been removed.

5.2.32 Credit Redemption.

Available credits may be collected from the Player Interface by the patron by choosing to cash out at any time other than during:

a) A game being played;

b) Audit mode;

c) Any door open;

d) Test mode;

e) A credit meter or win meter incrementation, unless the entire amount is placed on the meters when the collect button is pressed; or

f) A payout or memory error condition.

The term "cash out" includes, but is not limited to, buttons that cash-out, collect ,print receipt, print ticket, or claim.

5.2.33 Cancel Credit.

If credits are collected, and the total credit value is greater than or equal to a specific limit (printer limit for printer games), the game shall lock up until the credits have been paid, and the handpay is cleared by an attendant.

5.2.34 Payment by Ticket Printers.

If the Player Interface has a printer that is used to make payments, the Player Interface may pay the patron by issuing a printed ticket. In addition, payment by ticket printers as a method of credit redemption must meet the following requirements:

a) The printer shall be located in a locked area of the Player Interface, which requires opening of the

main door to access, but the printer shall not be located in the logic area or the drop box. This requirement ensures that changing the paper does not require access to the drop (cash) or logic areas containing critical electronic components.

b) The Player Interface, in which the printer is housed, is linked to a ticket validation system, which records the ticket information. Validation approval or information shall come from the ticket validation system in order to validate tickets. Tickets may be validated at any location, as long as it meets the standards within this section.

c) Each Player Interface shall be designed so that if communication is lost, and validation information cannot be sent to the ticket validation system, there is an alternate method of payment. The validation system must be able to identify duplicate tickets, to prevent fraud.

d) The printer shall print on a ticket and must provide the ticket data to a ticket validation system that records the following information regarding each payout ticket printed:

    i) Casino name/site identifier;

    ii) Machine number;

    iii) Date and time (24 hour format which is understood by the local date/time format);

    iv) Alpha and numeric dollar amount of the ticket;

    v) Ticket sequence number;

    vi) Validation number;

    vii) Bar code or any machine readable code representing the validation number;

    viii) Type of transaction or other method or differentiating ticket types (assuming multiple ticket types are available); and

    ix) Indication of an expiration period from date of issue, or date and time the ticket will expire (24 hour format which is understood by the local date/time format).

e) If the taxation limit is reached on any single play when using a ticket printer, then the ticket must not be able to be redeemed at any place other than through human interaction.

f) The Player Interface shall either keep a duplicate copy or print only one copy to the patron but have the ability to retain the ticket out information within the cashless transaction log, to resolve patron disputes. In addition, a CNGC approved ticket validation system shall be used to validate the payout ticket, and the ticket information on the system shall be retained at least as long as the ticket is valid at that location.

g) A printer shall have mechanisms to allow the Player Interface to interpret and act upon the following conditions. Such conditions must disable the game, and produce an error condition,

requiring attendant intervention to resume play:

i) Out of paper/paper low (It is not necessary to lock up a game during a "paper low" condition.);

ii) Printer jam/failure; and

iii) Printer disconnected – it is permissible for the Player Interface to detect this error condition when the game tries to print.

5.2.35 ACCESS TO PLAYER INTERFACE METERS.

The software meter information shall only be accessible by an authorized person.

5.2.36 CREDIT METER.

The credit meter shall be maintained in credits or cash value. In addition, the meter must meet the following, where applicable:

a) Progressives may be added to the credit meter if either:

i) The credit meter is maintained in the local currency amount; or

ii) The progressive meter is incremented to whole credit amounts; or

iii) The prize in the local currency amount is converted to credits on transfer to the patron's credit meter in a manner that does not mislead the patron (i.e., make unqualified statement "wins meter amount" and then rounds down on conversion) or cause accounting imbalances.

b) Residual Credits. If the current local currency amount is not an even multiple of the tokenization factor for a game or the credit amount has a fractional component, the won credits displayed for that game may be displayed and played as a truncated amount, (i.e., fractional part removed). However, the fractional credit information shall be made available to the patron when the truncated credit balance is zero. The fractional amount is also known as "residual credits." If residual credits exist, the manufacturer may provide a residual credit removal feature or allow a cancel credit or ticket print to remove the residual credits or return the Player Interface to normal game play (i.e., leave the residual credits on the patron's credit meter for betting). In addition:

i) Residual credits bet on the residual credit removal play shall be added to the coins-in (or cash in) meter;

ii) If the residual credit removal play is won, the value of the win shall either:

A. Increment the patron's credit meter; or

B. Be automatically dispensed, and the value of the coin(s) added to the coins-out (or cash out) meter.

iii) All other appropriate Player Interface meters (e.g., hopper level) shall be appropriately updated;

iv) If the residual credit removal play is lost, all residual credits are to be removed from the credit meter;

v) If the residual credits are cancelled rather than wagered, the Player Interface shall update the relevant meters (e.g., cancelled credit) and the last play information;

vi) The residual credit removal play feature shall return at least the minimum payback percentage, if one is set;

vii) The patron's current options and/or choices shall be clearly indicated electronically or by video display. These options shall not be misleading;

viii) If the residual credit removal play offers the patron a choice to complete the game (e.g., select a hidden card), the patron shall also be given the option of exiting the residual credit removal mode and returning to the previous mode;

ix) It shall not be possible to confuse the residual credit removal play with any other game feature (e.g., double-up or gamble);

x) If the residual credit removal play is offered on a multi-game Player Interface, the play shall (for meter purposes of each individual game) either be considered to be a part of the game from which the play was invoked, or be treated as a separate game; and

xi) The last game recall shall either display the residual credit removal play result or contain sufficient information (e.g., updated meters) to derive the result.

5.2.37 ELECTRONIC ACCOUNTING AND OCCURRENCE METERS.

Electronic accounting meters shall be at least seven (7) digits in length. If the meter is being used in dollars and cents, at least eight (8) digits must be used for the dollar amount. The meter must roll over to zero upon the next occurrence, any time the meter is seven (7) digits or higher and after 9,999,999 has been reached or any other value that is logical. Occurrence meters shall be at least eight (8) digits in length and roll over to zero upon the next occurrence, any time the meter is higher than the maximum number of digits for that meter. All gaming devices shall be equipped with a device, mechanism or method for retaining the value of all meter information which must be preserved in the event of power loss to the gaming device. The required electronic meters are as follows (accounting meters are designated with an asterisk "*"):

a) Coin In Meter: The electronic game shall have a meter that accumulates the total value of all wagers, whether the wagered amount results from the insertion of all approved financial instruments, deduction from a credit meter or any other means. This meter shall:

i) Not include subsequent wagers of intermediate winnings accumulated during game play sequence such as those acquired from "double up" games;

ii) Multi-game and multi-denominational electronic games shall be required to provide the information necessary, on a per paytable basis, to calculate a weighted average theoretical payback percentage; and

iii) Electronic games which contain paytables with a difference in theoretical payback percentage which exceeds 4 percent between wager categories, shall be required to maintain and display coin in meters and the associated theoretical payback percentage, for each wager category with a different theoretical payback percentage and calculate a weighted average theoretical payback percentage for that paytable;

b) Coin Out Meter: The electronic game must have a meter that accumulates the total value of all amounts directly paid by the electronic game as a result of winning wagers, whether the payout is made from the hopper to a credit meter or by any other means. This meter shall not record amounts awarded as the result of an external bonusing system or a progressive payout;

c) Attendant Paid Jackpots Meter: The electronic game shall have a meter that accumulates the total value of credit paid by an attendant resulting from a single winning alignment, combination or pattern for the amount of which is not capable of being paid by the electronic game itself. This does not include progressive amounts or amounts awarded as a result of an external bonusing system. This meter is only to include awards resulting from a specifically identified amount listed in the manufacturer's par sheet;

d) Cancelled Credits Meter: The electronic game shall have a meter that accumulates the total value paid by an attendant resulting from a patron initiated cash-out that exceeds the physical or configured capability of the electronic game to make the proper payout amount;

e) Bill In Meter: The electronic game shall have a meter that accumulates the total value of currency accepted. Additionally, the electronic game shall have a specific meter for each denomination of currency accepted that records the number of bills accepted of each denomination;

f) Ticket/Voucher In Meter: The electronic game shall have a meter that accumulates the total value of all electronic game wagering vouchers accepted by the electronic game;

g) Ticket/Voucher Out Meter: The electronic game shall have a meter that accumulates the total value of all electronic game wagering vouchers and payout receipts issued by the electronic game;

h) Electronic Funds Transfer In Meter (EFT In): The electronic game shall have a meter that accumulates the total value of cashable credits electronically transferred from an OMS to the electronic game when using EFT commands in the function of bonusing, promotions or cashless wagering;

i) Cashless Account Transfer In Meter (AFT In): The electronic game shall have a meter that accumulates the total value of cashable credits electronically transferred to the electronic game from a wagering account by means of an external connection between the electronic game and a cashless wagering system;

j) Cashless Account Transfer Out Meter: The electronic game shall have a meter that accumulates the total value of cashable credit electronically transferred from the electronic game to a wagering account by means of an external connection between the electronic game and a cashless wagering system;

k) Non-Cashable Electronic Promotion In Meter: The electronic game shall have meter that accumulates the total value of non-cashable credits electronically transferred to the electronic game from a promotional account by means of an external connection between the electronic game and a cashless wagering system;

l) Cashable Electronic Promotion In Meter: The electronic game shall have a meter that accumulates the total value of cashable credits electronically transferred to the electronic game from a promotional account by means of an external connection between the electronic game and a cashless wagering system;

m) Non-Cashable Electronic Promotion Out Meter: The electronic game shall have meter that accumulates the total value of non-cashable credits electronically transferred from the electronic game to a promotional account by means of an external connection between the electronic game and a cashless wagering system;

n) Cashable Electronic Promotion Out Meter: The electronic game shall have a meter that accumulates the total value of cashable credits electronically transferred from the electronic game to a promotional account by means of an external connection between the electronic game and a cashless wagering system;

o) Coupon Promotion In Meter: The electronic game shall have a meter that accumulates the total value of all electronic game coupons accepted by the electronic game;

p) Coupon Promotion Out Meter: The electronic game shall have a meter that accumulates the total value of all electronic game coupons issued by the electronic game;

q) Electronic Game Paid External Bonus Payout: The electronic game shall have a meter that accumulates the total value of additional amounts awarded as a result of an external bonusing system and paid by the electronic game;

r) Attendant Paid External Bonus Payout Meter: The electronic game shall have a meter that accumulates the total value of amounts awarded as a result of an external bonusing system paid by an attendant;

s) Attendant Paid Progressive Payout Meter: The electronic game shall have a meter that accumulates the total value of credits paid by an attendant as a result of progressive awards that are not capable of being paid by the electronic game itself;

t) Electronic Game Paid Progressive Payout Meter: The electronic game shall have a meter that accumulates the total value of credits paid as a result of progressive awards paid directly by the electronic game. This meter does not include awards paid as a result of an external bonusing system; and

u) Games played meter: The electronic game shall have meters that accumulate the number of games played for each of the following:

   i) Since power reset;

   ii) Since door close; and

   iii) Since game initialization (RAM clear);

v) External Doors Meter: The electronic game shall have a meter that accumulates the number of times the external cabinet door is opened which allows access to the logic area or financial instrument compartment which has been opened since the last RAM clear;

w) Required Progressive Meter: The electronic game shall have a meter that accumulates the number of times each progressive meter is activated.

x) Other Required Meter: The electronic game shall have a meter that accumulates the number of times the financial instrument validator door has been opened since the last RAM clear;

5.2.38 Multi-Game Game Specific Meters.

In addition to the electronic accounting meters required above, each individual game available for play shall have at least "amount bet" and "amount won" meters in either credits or dollars. Even if a "double-up or gamble" game is lost, the initial win amount/credits bet amount shall be recorded in the game specific meters. Alternatively, there can be separate meters that account for the double-up or gamble information. Either way, the method of metering must be understood on the screen.

5.2.39 Double-Up or Gamble Meters.

For each type of double-up or gamble offered, there shall be two meters to indicate the amount doubled and the amount won, which should increment every time a double-up or gamble occurs. If the Player Interface does not supply accounting for the double-up or gamble information, the feature must not be enabled for use.

5.2.40 Cashless Transaction Log.

All Player Interfaces must have the capacity to display a complete transaction history for the most recent transaction with a cashless wagering system (this would include tickets, coupons, electronically transferred promotional and/or bonusing credits, etc.), and the previous thirty-four transactions prior to the most recent transaction, that incremented any of the accounting meters.

5.2.41 Error Conditions.

Player Interfaces shall have the ability to produce a PIC, which shall be cleared either by an attendant or

upon initiation of a new play sequence and be communicated to an on-line monitoring and control system. The following errors, when applicable, must be detected and displayed:

a) RAM error;

b) Low RAM battery (for batteries external to the RAM itself or low power source);

c) Program error or authentication mismatch;

d) Door open (including bill acceptor);

e) Reel spin errors, including a mis-index condition for rotating reels, that affects the outcome of the game:

    i) The specific reel number shall be identified in the error code;

    ii) In the final positioning of the reel, if the position error exceeds one-half of the width of the smallest symbol excluding blanks on the reel strip; and

    iii) Microprocessor-controlled reels shall be monitored to detect malfunctions such as a reel which is jammed, or is not spinning freely, or any attempt to manipulate their final resting position.

f) Power reset;

g) Any credits on the Player Interface that are attempted to be transferred to the host system that result in a communication failure for which hand-pay is the only available payout medium (the patron cannot cashout via hopper or ticket printer) must result in a lockup or tilt on the Player Interface.

NOTE: For games that use error codes, a description of Player Interface error codes and their meanings shall be affixed inside the Player Interface. This does not apply to video-based games; however, video-based games shall display meaningful text as to the error conditions.

5.2.42 GAME INTERRUPTION AND RESUMPTION.

After a program interruption (e.g., power down), the software shall be able to recover to the state it was in immediately prior to the interruption occurring and:

a) If a Player Interface is powered down while in an error condition, then upon restoring power, the error message shall be displayed and the Player Interface shall remain locked-up. This is unless power-down is used as part of the error reset procedure, or if on power-up or door closure, the Player Interface checks for the error condition and detects that the error is no longer in existence.

b) Upon program resumption, the following procedures shall be performed as a minimum requirement:

    i) Any communications to an external device shall not begin until the program resumption routine, including self-tests, is completed successfully;

ii) Player Interface control programs shall test themselves for possible corruption due to failure of the program storage media. The authentication may use the checksum; however, it is preferred that the cyclic redundancy check calculations are used as a minimum (at least 16 bit). Other test methodologies shall be of a certified type;

iii) The integrity of all critical memory shall be checked; and

iv) Games utilizing microprocessor controlled mechanical displays (e.g., reels or wheels), shall re-spin automatically to display the last valid game's result when the play mode is re-entered, and the reel positions have been altered.

5.2.43 DOOR OPEN EVENTS.

When the Player Interface's main door is opened, the game shall cease play, enter an error condition, display an appropriate error message, disable coin acceptance and bill acceptance, and initiate a PIC. When the Player Interface's main door is closed, the game shall return to its original state and display an appropriate error message, until the next game has ended. The software shall be able to detect any meter access to the following doors or secure areas:

a) All external doors;

b) Stacker door; and

c) Bill acceptor door.

5.2.44 GAME CYCLE.

A game is considered completed when the final transfer to the patron's credit meter takes place (in case of a win), or when all credits wagered or won that have not been transferred to the credit meter, are lost.

a) The following are all considered to be part of a single game:

i) Games that trigger a free game feature and any subsequent free games;

ii) "Second screen" bonus feature(s);

iii) Games with patron choice (e.g., poker or blackjack);

iv) Games where the rules permit wagering of additional credits (e.g., blackjack insurance); and

v) Double-up/gamble features.

5.2.45 RNG REQUIREMENTS.

Where the authorized game or system uses a RNG to make selections, such RNG and the selections shall:

a) Be statistically independent;

b) Conform to the desired random distribution;

c) Pass various recognized statistical tests;

d) Be unpredictable;

e) Be cycled continuously in the background between games and during game play at a speed that cannot be timed by the patron.

f) Randomly determine the first seed by an uncontrolled event. After every game, there shall be a random change in the RNG process (new seed, random timer, delay, etc.). This will verify the RNG does not start at the same value, every time. It is permissible not to use a random seed; however, the manufacturer must ensure that the games will not synchronize. The ITL shall verify that the games will not synchronize.

g) If a random number with a range shorter than that provided by the RNG is required for some purpose within the Player Interface, the method of re-scaling (i.e., converting the number to the lower range) is to be designed in such a way that all numbers within the lower range are equally probable.

h) If a particular random number selected is outside the range of equal distribution of re-scaling values, it is permissible to discard that random number and select the next in sequence for the purpose of re-scaling.

i) Unless otherwise denoted on the payglass, where the Player Interface plays a game that is recognizable, such as poker, blackjack, etc., the same probabilities associated with the live game shall be evident in the simulated game. For example, the odds of drawing a specific card or cards in poker shall be the same as in the live game as if a physical deck of cards were being used. Card games also must meet the following:

    i) Cards once removed from the deck shall not be returned to the deck except as provided by the rules of the game depicted; and

    ii) As cards are removed from the deck they shall be immediately used as directed by the rules of the game (i.e., the cards are not to be discarded due to adaptive behavior by the Player Interface).

j) Where used, mechanical based RNG games are games that use the laws of physics to generate the outcome of the game. All mechanical based RNG games must meet the requirements of these Uniform Standards with the exception of the requirement stated above that dictate the requirements for electronic RNGs.

NOTE: As a part of the test results, the ITL will advise the CNGC, to the degree it can, if any of the parts of the device are subject to deterioration so that the regulator can take appropriate action.

k) Each possible permutation or combination of game elements that produces winning or losing game outcomes shall be available for random selection at the initiation of each play, unless otherwise denoted by the game.

l) A Player Interface shall use appropriate communication protocols to protect the RNG and random selection process from influence by associated equipment, which may be communicating with the Player Interface.

5.2.46 Software Requirements for Percentage Payout.

Each game shall theoretically pay out a minimum of 75% during the expected lifetime of the game. The game's patron return over the cycle of both the bonus and non-bonus part of the game shall conform to the minimum theoretical return to patron. In addition, the game must meet the following requirements:

a) Optimum Play Used for Skill Games. Player Interfaces that may be affected by patron skill shall meet the percentage payout requirement, provided one is set, when using a method of play that will provide the greatest return to the patron over a period of continuous play.

b) Minimum Percentage Requirement Met at All Times. The minimum percentage requirement shall be met at all times. The minimum percentage requirement shall be met when playing at the lowest end of a non-linear paytable (i.e., if a game is continuously played at a minimum bet level for its total game cycle and the theoretical RTP is lower than the minimum percentage, then the game is unacceptable).

c) Double-up or Gamble. The double-up or gamble options shall have a theoretical return to the patron of one hundred percent (100%) unless otherwise noted to the patron. The ITL shall provide the minimum and maximum theoretical payout percentage within the certification report. Additional awards added to a game will require a re-evaluation of the theoretical payout percentage, considering the value of the award and possibly other factors. The ITL will re-evaluate a game's theoretical payout percentage when requested.

5.2.47 Multiple Percentages.

For games that offer multiple percentages, please refer to Section 5.2.13 Configuration Setting requirements of these Uniform Standards. For games connected by a network, security measures will be reviewed by the CNGC on a case-by-case basis.

5.2.48 Merchandise Prizes in Lieu of Cash Awards.

Limitations (annuities – lump sum or periodic payments) on the prize amount of merchandise shall be clearly explained to the patron on the game that is offering such a prize.

5.2.49 Bonus Games.

If the game contains a "bonus feature," including a game within a game, the following requirements shall be met:

a) The game shall display clearly to the patron which game rules apply to the current game state;

b) Extended feature information: Each electronic game, which offers an extended feature (e.g., free games, re-spins, etc.), must display the number of feature games that remain during each game; except for extended features that are predetermined by the system (e.g., Class II server based systems);

c) The game, other than those that occur randomly, shall display to the patron sufficient information to indicate the current status towards the triggering of the next bonus game (i.e., if the game requires obtaining several events/symbols towards a feature, the number of events/symbols needed to trigger the bonus shall be indicated along with the number of events/symbols collected at any point);

d) The game shall not adjust the likelihood of a bonus occurring, based on the history of prizes obtained in previous games (i.e., games shall not adapt their theoretical return to patron based on past payouts);

e) If a bonus or feature game requires extra credits to be wagered and the game accumulates all winnings (from the trigger and the feature) to a temporary "win" meter (rather than directly to the credit meter), the game shall:

    i) Provide a means where winnings on the temporary meter can be bet (via the credit meter) to allow for instances where the patron has an insufficient credit meter balance to complete the feature;

    ii) Transfer all credits on the temporary meter to the credit meter upon completion of the feature;

    iii) Not exceed the max bet limit, if one is set; and

    iv) Provide the patron an opportunity not to participate.

f) If a game's bonus is triggered after accruing a certain number of events/symbols or combination of events/symbols of a different kind, the probability of obtaining like events/symbols shall not deteriorate as the game progresses (e.g., for identical events/symbols it is not permitted that the last few events/symbols needed are more difficult to obtain than the previous events/symbols of that kind);

g) The game shall make it clear to the patron that they are in this mode to avoid the possibility of the patron walking away from the Player Interface not knowing the game is in a bonus mode; and

h) Games that have an award calculated, occurring from game play within the base game's cycle made upon the completion of a series of random occurrences, shall meet the following:

    i) Extended play awards are part of the game cycle with predetermined award values. Extended play award contributions to the program payout percentage are calculated consistent with awards of the regular game cycle. Specifically, if the cycle for extended play awards is different from the base game cycle, then the extended play awards, occurring within the base game's cycle, will be calculated as part of the game's payout; and

ii) Pursuant to the rules, the game shall display the rules of play for the extended play awards, the rewards associated with each extended play award, and the character combinations that will result in specific payouts. For extended play awards achieved by obtaining specific game results, the progress of the award shall be displayed.

5.2.50 MULTI-LINE GAMES.

Each individual line to be played shall be clearly indicated by the Player Interface so that the patron is in no doubt as to which lines are being bet on. In addition, the winning playline(s) shall be clearly discernable to the patron. (For example, on a video game, it may be accomplished by drawing a line over the symbols on the playline(s) and/or the flashing of winning symbols and line selection box. Where there are wins on multiple lines, each winning playline may be indicated in turn. This would not apply to games that use mechanical reels.)

5.2.51 MULTIPLE GAMES OFFERED FOR PLAY AT ONE PLAYER INTERFACE.

The following requirements apply to Player Interfaces that offer more than one (1) game to be played:

a) The methodology employed by a patron to select and discard a particular game for play on a multi-game Player Interface shall be clearly explained to the patron on the Player Interface and be easily followed.

b) The Player Interface shall be able to clearly inform the patron of all games, their rules and/or the paytables before the patron must commit to playing them.

c) The patron shall at all times be made aware of which game has been selected for play and is being played.

d) The patron shall not be forced to play a game just by selecting that game. The patron shall be able to return to the main menu.

e) It should not be possible to start a new game before the current play is completed and all relevant meters have been updated (including features, gamble and other options of the game).

f) The set of games offered to the patron for selection, or the paytable, can be changed only by a secure certified method which includes turning on and off games available for play through the Player Interface. The requirements outlined in Section 5.2.13 Configuration Setting of these Uniform Standards shall govern the RAM Clear control requirements for these types of selections. However, for games that keep the previous paytable's data in memory, a RAM clear is not required.

g) No changes to the set of games offered to the patron for selection (or to the paytable) are permitted while there are credits on the patron's credit meter or while a game is in progress.

5.2.52 TAXATION REPORTING LIMITS.

The game shall be capable of entering a lock-up condition if the sum of awards from a single game is equal to the then current taxation limit and shall require an attendant to clear.

5.2.53 TEST/DIAGNOSTIC MODE (DEMO MODE).

If in a test mode, the game shall clearly indicate that it is in a test mode, not normal play, and:

a) Any test that incorporates credits entering or leaving the Player Interface shall be completed on resumption of normal operation;

b) There shall not be any test mode that increments any of the electronic meters (test meters are permissible provided the meter indicates as such);

c) Any credits on the Player Interface that were accrued during the test mode shall be cleared before the test mode is exited;

d) The following conditions shall automatically place the Player Interface into a service or test mode:

    i) main cabinet door open, or

    ii) during audit mode access; and

e) When exiting from test mode, the game shall return to the original state it was in when the test mode was entered.

5.2.54 NUMBER OF LAST PLAYS REQUIRED.

Information on at least the last ten games is to always be retrievable on the operation of a suitable external key-switch, or another secure method that is not available to the patron. Last play information shall provide all information required to fully reconstruct the last ten plays. All values shall be displayed, including the initial credits, credits bet, credits won, and credits paid. If a progressive was awarded, it is sufficient to indicate the progressive was awarded and not display the value. This information should include the final game outcome, including all patron choices and bonus features. The results of double-up or gamble (if applicable) should also be included. The last game recall shall reflect bonus rounds in their entirety. If a bonus round lasts "x number of events," each with separate outcomes, each of the "x events" shall be displayed with its corresponding outcome if the outcome results in an award. The recall shall also reflect position-dependent events if the outcome results in an award. For games that may have infinite free games, there shall be a minimum of fifty games recallable.

5.2.55 SOFTWARE VERIFICATION.

The device shall have the ability to allow for an independent integrity check of the device's software from an outside source. This must be accomplished by being authenticated by a third-party device, which may be embedded within the game software or having an interface port for a third-party device to authenticate the media. This integrity check will provide a means for field testing the software to identify and validate the program. The ITL, prior to device approval, shall approve the integrity check method. If the authentication program is contained within the game software, the manufacturer must receive written approval from the ITL prior to submission.

CHAPTER 6

ONLINE ACCOUNTING SYSTEM REQUIREMENTS

6.1 INTRODUCTION

6.1.1 INTRODUCTION.

This section reflects additional requirements that, while not specifically required by the Compact, have been determined by the CNGC as being necessary to meet the Tribe's standards for electronic gaming. All electronic games sought to be played in a Choctaw Nation of Oklahoma gaming facility pursuant to the Compact and 25 CFR Part 547 shall meet these additional requirements. It should be noted that all of these standards shall be met "where applicable" (e.g., if the device does not have a mechanical display, adherence to "mechanical display" requirements are not required).

6.2 ON-LINE SYSTEM

6.2.1 INTRODUCTION.

The regulations within this section are primarily "general" computer system, requirements that apply equally to an On-Line Monitoring Control System (MCS) and any other system that would have an effect on critical accounting or security information, such as a ticket validation system, promotional, or bonusing system, unless the system type is specifically noted.

6.2.2 INTERFACE ELEMENTS.

An interface element, where applicable, is any component within a system that is external to the operations of the Player Interface, that assists in the collection and processing of data, and that is sent to a system. All critical interface elements shall:

a) Be installed in a secure area (which may be inside a Player Interface).

b) The interface element setup/configuration menu(s) must not be available unless using an authorized access method.

c) If not directly communicating with Player Interface meters, the interface element must maintain separate electronic meters, of sufficient length, to preclude the loss of information from meter rollovers, or a means to identify multiple rollovers, as provided for in the connected Player Interface. These electronic meters should be capable of being reviewed on demand at the interface element level via an authorized access method.

d) The interface element must retain the required information after a power loss for a period determined by the CNGC. If this data is stored in volatile RAM, a battery backup must be installed within the interface element.

e) If unable to communicate the required information to the MCS, the interface element must provide a

means to preserve all mandatory meter and significant event information until such time as it can be communicated to the MCS. Player Interface operation may continue until critical data is overwritten and lost. There must be a method to check for corruption of the above data storage locations.

f) The interface element must allow for the association of a unique identification number to be used in conjunction with a Player Interface file on the MCS. This identification number will be used by the MCS to track all mandatory information of the associated Player Interface. Additionally, the MCS should not allow for a duplicate Player Interface file entry of this identification number.

g) A MCS may possess a front end processor that gathers and relays all data from the connected data collectors to the associated database(s). The data collectors, in turn, collect all data from, connected Player Interfaces. Communication between components must be a defined communication protocol(s) and function as indicated by the communication protocol(s). A MCS must provide for the following:

    i) All critical data communication shall be protocol based and/or incorporate an error detection and correction scheme to ensure an accuracy of ninety-nine percent (99%) or better of messages received; and

    ii) All critical data communication that may affect revenue and is unsecured either in transmission or implementation shall employ encryption. The encryption algorithm shall employ variable keys or similar methodology to preserve secure communication.

NOTE: These standards do not preclude the use of RF technology in any of the system components, provided all security issues are addressed.

6.2.3 SYSTEM SERVER(S).

System server(s), networked system(s) or distributed system(s) that directs the overall operation and an associated database(s) that stores all entered and collected system information, is considered the "server." In addition, the server shall:

a) Maintain an internal clock that reflects the current time (24-hour format - which is understood by the local date/time format) and data that shall be used to provide for the following:

    i) Time stamping of significant events;

    ii) Reference clock for reporting;

    iii) Time stamping of configuration changes;

    iv) If multiple clocks are supported the MCS shall have a facility whereby it is able to update those clocks in MCS components, where conflicting information could occur.

b) Electronic Bonanza-Style Bingo Game Specific. The on-line monitoring and/or game server shall be capable of maintaining the following accounting and event data and shall be capable of producing reports on demand:

i) Data required to be maintained for each Electronic Bonanza-Style Bingo Game includes:

A. Date and time of the game start and game end;

B. Cards-in-play count by location;

C. Identification number of winning card(s);

D. Ordered list of balls or numbers drawn;

E. Prize amounts awarded for each game, for each location/Player Interface; and

F. All information for special games that would be required to validate a bingo (i.e., color, special patterns, special cards, free strips, odd/even numbers, etc.).

ii) Sales information for each bingo game shall include:

A. The name of the organization or hall;

B. Price of card faces;

C. Daily sales totals, by location;

D. Game-by-game sales and prizes by location;

E. Packet Sales. There shall be an easy means to determine the specific cards sold for play, for each game. Daily reports based on the calendar date must provide this information;

F. Daily network summary, by game and by location (applies to multiple sites using a single server);

G. Cash due and cash received reconciliation; and

H. Hard/soft count reconciliation which is a log of all accounting changes (i.e., meter adjustments and sales data corrections) including the employee name/ID authorized to make the changes, the date of the change, the time of the change, and the detailed items adjusted shall be kept on the system.

6.2.4 JACKPOT/FILL FUNCTIONALITY.

A Monitoring and Control Systems (MCS) must have an application or facility that captures and processes every handpay message from each Player Interface and meet the following requirements:

a) Handpay messages must be created for single wins (jackpots), progressive jackpots, and accumulated credit cash outs (canceled credits) that result in handpays.

b) For every single win event that is equal to or greater than the then current taxation limit, the user must be advised of the need for a W2G or 1042S (if applicable) to be processed, either via the MCS or manually. This option must not be capable of being overridden. The keyed reset ability to return winnings from a taxable event to a Player Interface should require user intervention to void the original jackpot slip that is generated.

c) The following information is required for all slips generated by the MCS:

   i) Type of slip;

   ii) Numeric slip identifier (which increments per event);

   iii) Date and time (Shift if required);

   iv) Player Interface number;

   v) Denomination;

   vi) Amount of fill;

   vii) Amounts of jackpot, accumulated credit, and additional pay; W2G indication, if applicable;

   viii) Additional payout, if applicable;

   ix) Total before taxes and taxes withheld, if applicable;

   x) Amount to patron;

   xi) Total played and game outcome of award;

   xii) Soft meter readings; and

   xiii) Relevant signatures as required.

NOTE: Some of the above may pertain to fill slips, jackpot slips, or both. The above information may vary dependent upon the jurisdictional internal controls and may or may not be required.

d) A fill (deposit of a predetermined or otherwise properly authorized, token amount in a Player Interface's hopper) is normally initiated from a hopper empty message while a credit (removal of excess tokens from a Player Interface) is normally user initiated. An allowable exception to fill initiation would be where the system provides preventative or maintenance fill functionality, in which the transaction may be initiated by the system or an authorized user. Once captured, there must be adequate access controls to allow for authorization, alteration, or deletion of any of the values prior to payment or execution.

6.2.5 REQUIRED MCS FUNCTIONALITY.

At a minimum, an MCS shall provide for the following security and auditability requirements:

a) An interrogation program that enables on-line comprehensive searching of the significant event log for the present and for the previous 14 days through archived data or restoration from backup where maintaining such data on a live database is deemed inappropriate. The interrogation program shall have the ability to perform a search based at least on the following:

    i) Date and time range;

    ii) Unique interface element /Player Interface identification number; and

    iii) Significant event number/identifier.

b) A MCS must have a master "Player Interface" which is a database of every Player Interface in operation, including at minimum the following information for each entry:

    i) Unique interface element /location identification number;

    ii) Player Interface identification number as assigned by the casino;

    iii) Denomination of the Player Interface (please note that the denomination may reflect an alternative value, in the case of a multi-denomination game);

    iv) Theoretical hold of the Player Interface; and

    v) Control program(s) within Player Interface.

If the MCS retrieves any of these parameters directly from the Player Interface, sufficient controls must be in place to ensure accuracy of the information.

c) Significant events are generated by a Player Interface and sent via the interface element to the MCS utilizing an approved communication protocol. Each event must be stored in a database(s), which includes the following:

    i) Date and time which the event occurred;

    ii) Identity of the Player Interface that generated the event;

    iii) A unique number/code that defines the event; and

    iv) A brief text that describes the event in the local language.

d) The following are the significant events that must be collected from the Player Interface and transmitted to the system for storage.

    i) Power resets or power failure.

ii) Handpay conditions (amount needs to be sent to the system):

A. Player Interface jackpot (an award in excess of the single win limit of the Player Interface);

B. Progressive jackpot (as per jackpot above).

iii) Door openings (any external door, that accesses a critical area, on the Player Interface).

iv) Door switches (discrete inputs to the interface element) are acceptable if their operation does not result in redundant or confusing messaging.

e) Bill (item) acceptor errors ("i" and "ii" should each be sent as a unique message, if supported by the communication protocol):

i) Stacker full (if supported); and

ii) Bill (item) jam.

f) Player Interface low RAM battery error.

g) Reel spin errors (if applicable with individual reel number identified).

h) Printer errors (if printer supported):

i) Printer empty/paper low; and

ii) Printer disconnect/failure.

i) The following priority events must be conveyed to the MCS where a mechanism must exist for timely notification:

i) Loss of communication with interface element;

ii) Loss of communication with Player Interface;

iii) Memory corruption of the interface element, if storing critical information; and

iv) RAM corruption of the Player Interface.

6.2.6 MCS STORED ACCOUNTING METERS.

Metering information is generated on a Player Interface and collected by the interface element and sent to the MCS via a communication protocol. This information may be either read directly from the Player Interface or relayed using a delta function. The MCS must collect and store the following meter information from each Player Interface:

a) Total in (credits-in);

b) Total out (credits-out);

c) Total dropped (coins-dropped or total value of all coins, bills and tickets dropped);

d) Hand paid (handpays);

e) Cancelled credits (if supported on Player Interface);

f) Bills in (total monetary value of all bills accepted);

g) Individual bill meters (total number of each bill accepted per denomination);

h) Games-played;

i) Cabinet door (instance meter which may be based on MCS count of this event);

j) Drop door(s) (instance meter which may be based on MCS count of this event);

k) Tickets in (total monetary value of all tickets accepted); and

l) Tickets out (total monetary value of all tickets produced).

The Player Interface software electronic accounting and occurrence metering requirements provide more detailed descriptions of the above meters. While these electronic accounting meters should be communicated directly from the Player Interface to the MCS, it is acceptable to use secondary MCS calculations where appropriate.

6.2.7 MCS Required Reports.

Reports will be generated on a schedule determined by the CNGC, which typically consists of daily, monthly, yearly period, and life to date reports generated from stored database information. These reports at minimum will consist of the following:

a) Net win/revenue report for each Player Interface;

b) Drop comparison reports for each medium dropped (examples = tickets, bills) with dollar and percent variances for each medium and aggregate for each type;

c) Metered vs. actual jackpot comparison report with the dollar and percent variances for each and aggregate;

d) Theoretical hold vs. actual hold comparison with variances;

e) Significant event log for each Player Interface; and

f) Other reports, as required by the CNGC.

NOTE: It is acceptable to combine reporting data where appropriate (e.g., revenue, theoretical/actual comparison).

NOTE: For additional revenue reporting requirements when ticket drop Player Interfaces are interfaced, please see "Ticket Validation System Requirements," below.

6.2.8 Security Access Control.

The MCS must support either a hierarchical role structure whereby user and password define program or individual menu item access or logon program/device security based strictly on user and password or PIN. In addition, the MCS shall not permit the alteration of any significant log information communicated from the Player Interface. Additionally, there should be a provision for system administrator notification and user lockout or audit trail entry, after a set number of unsuccessful login attempts.

6.2.9 Data Alteration.

The MCS shall not permit the alteration of any accounting or significant event log information that was properly communicated from the Player Interface without supervised access controls. In the event financial data is changed, an audit log must be capable of being produced to document:

a) Data element altered;

b) Data element value prior to alteration;

c) Data element value after alteration;

d) Time and Date of alteration; and

e) Personnel that performed alteration (user login).

6.2.10 System Back-Up.

The system(s) shall have sufficient redundancy and modularity so that if any single component or part of a component fails, gaming can continue. There shall be redundant copies of each log file or system database or both, with open support for backups and restoration.

6.2.11 Recovery Requirements.

In the event of a catastrophic failure when the system(s) cannot be restarted in any other way, it shall be possible to reload the system from the last viable backup point and fully recover the contents of that backup, recommended to consist of at least the following information:

a) Significant Events;

b) Accounting information;

c) Auditing information; and

d) Specific site information such as device file, employee file, progressive set-up, etc.

6.2.12 Verification of Player Interface Software via the System.

If supported, system(s) may provide this redundant functionality to check Player Interface game software. Although the overhead involved can potentially impede Player Interface and operation, the following information must be reviewed for validity prior to implementation:

a) Software signature algorithm(s); and

b) Data communications error check algorithm(s).

6.2.13 Download Requirements.

If supported and permitted, a MCS may utilize writable program storage technology to update interface element software if all of the following requirements are met:

a) Writable program storage functionality must be, at a minimum, password-protected, and should be at a supervisor level. The MCS can continue to locate and verify versions currently running but it cannot load code that is not currently running on the system without user intervention;

b) A non-alterable audit log must record the time/date of a writable program storage download and some provision must be made to associate this log with which version(s) of code was downloaded, and the user who initiated the download. A separate download audit log report is ideal;

c) All modifications to the download executable or other file(s) must be submitted to the ITL for approval. The ITL will assign signatures to any relevant executable code and file(s) that should be verified by a regulator in the field. Additionally, all downloadable files must be available to a regulator to verify the signature; and

d) The system must have the ability to verify the program on demand for regulatory audit purposes. This rule refers to loading of new system executable code only. Other program parameters may be updated as long as the process is securely controlled and subject to audit. The parameters must be reviewed on an individual basis.

6.2.14 Remote Access Requirements.

If supported, system(s) may utilize password controlled remote access, provided the following requirements are met:

a) A “remote access user activity” log is maintained depicting logon name, time/date, duration, activity while logged in;

b) No unauthorized remote user administration functionality (adding users, changing permissions, etc.);

c) No unauthorized access to database other than information retrieval using existing functions;

d) No unauthorized access to operating system; and

e) If remote access is to be on a continuous basis, then a network filter (firewall) should be installed to protect access.

NOTE: The MCS manufacturer may, as needed, remotely access the MCS and its associated components for the purpose of product and user support. However, this feature must be optional, by a secure means, to accommodate locations that do not permit or want to regulate system access.

6.3 TICKET VALIDATION SYSTEM — ADDITIONAL REQUIREMENTS

6.3.1 GENERAL STATEMENT.

A ticket validation system may be entirely integrated into a MCS or exist as an entirely separate entity. Payment by ticket printer as a method of credit redemption on a Player Interface is only permissible when the Player Interface is linked to an approved ticket validation system. Validation information shall be communicated from the system to the Player Interface using a secure communication protocol. This section concerns bi-directional ticket validation system specific requirements where a ticket validation system that is independent of an MCS would also require the security and integrity standards previously outlined within this chapter.

6.3.2 TICKET INFORMATION.

A ticket shall contain the following printed information at a minimum:

a) Casino name/site identifier;

b) Machine number (or cashier/change booth location number or equivalent context, if ticket creation, outside the Player Interface, is supported);

c) Date and time (24-hour format which is understood by the local date/time format);

d) Alpha and numeric dollar amount of the ticket;

e) Ticket sequence number;

f) Validation number;

g) Bar code or any machine readable code representing the validation number;

h) Type of transaction or other method or differentiating ticket types (assuming multiple ticket types are available); and

i) Indication of an expiration period from date of issue, or date and time the ticket will expire (24-hour format which is understood by the local date/time format).

NOTE: Some of this information may be contained in the validation number.

6.3.3 TICKET TYPES.

If Player Interface ticket generation is to be supported while not connected to the validation system, a ticket system must generate two different types of tickets at minimum. On-line and off-line types are denoted respectively by ticket generation either when the validation system and Player Interface are properly communicating, or the validation system and Player Interface are not communicating properly. When a patron cashes out of a Player Interface that has lost communication with the validation system, the Player Interface must lock up and, after reset, may print an off-line ticket or handpay receipt. The ticket or handpay receipt must be visually distinct from an on-line ticket either in format or content while still maintaining all information required.

6.3.4 TICKET ISSUANCE.

A ticket can be generated at a Player Interface through an internal document printer, at a patron's request, by redeeming all credits. Tickets that reflect partial credits may be issued automatically from a Player Interface. Additionally, cashier/change booth issuance is allowed if supported by the validation system.

6.3.5 TICKET REDEMPTION.

Tickets may be inserted in any Player Interface participating in the validation system providing that no credits are issued to the Player Interface prior to confirmation of ticket validity. The customer may also redeem a ticket at a validation Interface (i.e., cashier/change booth, redemption Interface or other approved methods) All validation Interfaces shall be user and password-controlled. Where the validation is to take place at a cashier/change booth, the cashier shall:

a) Scan the bar code via an optical reader or equivalent; or

b) Input the ticket validation number manually; and

c) Shall be capable of printing a validation receipt, after the ticket is electronically validated. The validation receipt, at a minimum, shall contain the following printed information:

    i) Machine number;

    ii) Validation number;

    iii) Date and time paid;

    iv) Amount; and

    v) Cashier/change booth identifier.

6.3.6 INVALID TICKET NOTIFICATION.

The ticket validation system must have the ability to identify invalid tickets and notify the Player Interface to "reject" the ticket or advise the cashier that one of the following conditions exists:

a) Ticket cannot be found on file (stale date, forgery, etc.);

b) Ticket has already been paid; or

c) Amount of ticket differs from amount on file (requirement can be met by display of ticket amount for confirmation by cashier during the redemption process). In the event the amounts differ, the amount value on file shall take precedence.

6.3.7 Offline Ticket Redemption.

If the on-line data system temporarily goes down and validation information cannot be sent to the validation system, an alternate method of payment must be provided either by the validation system possessing unique features (e.g., validity checking of ticket information in conjunction with a local database storage) to identify duplicate tickets and prevent fraud by reprinting and redeeming a ticket that was previously issued by the Player Interface or by use of an approved alternative method as designated by the regulatory jurisdiction that will accomplish the same.

6.3.8 Required Reports.

The following reports shall be generated at a minimum and reconciled with all validated/redeemed tickets:

a) Ticket issuance report;

b) Ticket redemption report;

c) Ticket liability report;

d) Ticket drop variance report;

e) Transaction detail report must be available from the validation system that shows all tickets generated by a Player Interface and all tickets redeemed by the validation Interface or other Player Interface; and

f) Cashier report, which is to detail individual tickets, the sum of the tickets paid by cashier/change booth or redemption Interface.

NOTE: The requirements for "b" and "d" are waived where two-part tickets exist for the Player Interface, and where the first part is dispensed as an original ticket to the patron and the second part remains attached to the printer mechanism as a copy (on a continuous roll) in the Player Interface.

6.3.9 Security of Ticket Information.

Once the validation information is stored in the database, the data may not be altered in any way. The validation system database must be encrypted or password-protected and should possess a non-alterable user audit trail to prevent unauthorized access. Further, the normal operation of any device that holds ticket information shall not have any options or methods that may compromise ticket information. Any device that holds ticket information in its memory shall not allow removing of the information unless it has first transferred that information to the database or other secured component(s) of the validation system.

CHAPTER 7

TERMINAL/CLIENT-SERVER SYSTEM COMMUNICATION

7.1 COMMUNICATION REQUIREMENTS

7.1.1 COMMUNICATION PROTOCOL.

The Terminal/Client Server System (TCSS), terminals/clients and all interface elements within the Terminal/Client Server System environment shall function as indicated by the communication protocol implemented. Protocols shall use communication techniques that have proper error detection and/or recovery mechanism, which shall consist of encryption with secure seeds or algorithms. Any alternative measures shall require CNGC approval.

7.1.2 COMMUNICATIONS LOSS.

For a game system which is server based, a terminal/client shall be rendered unplayable if communications from the server or system portion of the terminal/client is lost. If a game is in progress, a mechanism shall be provided to recover to the point of the game when communication was lost. The CNGC may also alternatively approve in a multi-player environment that a loss of communication can result in aborting the game and refunding the patron's wager. For a terminal/client that has a loss of communication with the server, the TCSS shall provide a means to cash out credits indicated on the terminal/client at the time communication was lost.

7.2 TERMINAL/CLIENT SERVER SYSTEM SECURITY REQUIREMENTS

7.2.1 FIREWALL SECURITY.

A Terminal/Client Server utilized in conjunction with other networks or any communication which includes but is not limited to remote access, shall pass through at least one or more CNGC approved application(s) level firewall and shall not have any function which would allow for an alternate network path (unless redundancy purpose) without detection. In the event an alternate exists for redundancy purposes it shall also pass through at least one application level firewall approved by the CNGC.

Note: The Independent Testing Laboratory (ITL) shall provide any additional security recommendations within the lab certification. Onsite training shall be provided if requested by the CNGC.

7.2.2 FIREWALL AUDIT LOG.

The CNGC approved firewall application shall maintain at least the following information and shall disable all communication and generate an error report if the audit log becomes full:

a) Any firewall configuration changes;

b) Both successful and unsuccessful connection attempts through the firewall; and

c) If applicable, the source and destination IP Addresses, Port Numbers, and MAC Addresses.

7.3 REMOTE ACCESS REQUIREMENTS

7.3.1 REMOTE ACCESS SECURITY.

Remote access shall authenticate all computer systems based on the CNGC approved settings of the TCSS or firewall application that establishes a connection with the TCSS. The items below are additional Remote Access Security requirements:

a) Unauthorized remote user administration functionality shall not be allowed (ex. Adding users, changing permissions, etc.);

b) Unauthorized access to any database other than information retrieval using existing functions shall not be allowed; and

c) Unauthorized access to the operating system shall not be allowed.

Note: It is understood that the TCSS and associated software may need to be remotely accessed for the purpose of customer support. Any remote access shall follow a CNGC approved process.

7.3.2 REMOTE ACCESS AUDITING.

Either a TCSS or CNGC approved third party remote access software tool shall maintain an activity log which can either be automatically or have the ability to manually enter the logs showing all remote access information that includes at least the following information:

a) Log on Name;

b) Time and date the connection was made;

c) Duration of connection; and

d) All activity while logged-in

7.4 WIDE AREA NETWORK COMMUNICATION REQUIREMENTS

7.4.1 WIDE AREA NETWORK.

Wide Area Network (WAN) communication may be permitted for use within Choctaw Nation operated gaming facilities. The following shall be required of the WAN to be considered for use within a Choctaw Nation operated gaming facility:

a) Communication over the WAN shall be secure from intrusion, interference and snooping, via techniques such as the use of a Virtual Private Network (VPN), encryption, authentication etc.;

b) Functions documented in the communications protocol shall be the only functions allowed over the WAN. The protocol shall be provided to an ITL. The protocol documentation may be in multiple

parts; and

c) The TCSS in operation with multiple sites which are linked shall require CNGC Approval.

7.5 TERMINAL/CLIENT SERVER SYSTEM REQUIREMENTS

7.5.1 SERVER BASED SYSTEM.

The server shall generate and transmit to the terminal/client control, configuration and information data. Dependent upon the implementation within a Choctaw Nation operated gaming facility, examples include, but are not limited to:

a) Random numbers;

b) Game result components, e.g., reel stop positions;

c) Actual game results;

d) Credit movement; or

e) Updates to the credit meter for winning game outcomes.

7.5.2 SERVER SUPPORTED GAME SYSTEM.

A game server shall not participate in the game outcome determination process. The primary functions shall be that of downloading control programs and other software resources, or providing command and control instruction that may change the configuration of the software already loaded on the terminal/client, on an intermittent basis.

7.5.3 SECURITY.

Servers shall be housed in a secure locked cabinet outside of the terminal/client, secure data room, or other CNGC approved secure area.

7.5.4 INTRUSION PROTECTION.

Servers shall have logical intrusion protection against unauthorized access.

7.5.5 CONFIGURATION ACCESS.

The TCSS interface element setup/configuration menu(s) shall not be available unless using a secure authorized access method approved by the CNGC.

7.5.6 SERVER PROGRAMMING.

There shall be no means available for conducting programming on the server in any configuration (shall not be able to perform SQL statements to modify the database schema). A Network Administrator possessing a valid license with the CNGC may perform authorized network infrastructure maintenance (this includes the

use of SQL statements that already reside on the system) with sufficient access rights as required by the Choctaw Nation.

7.5.7 VIRUS PROTECTION.

The TCSS utilized within Choctaw Nation operated gaming facilities shall have CNGC approved virus protection.

7.5.8 COPY PROTECTION.

The implementation of copy protection to prevent unauthorized proliferation or modification of software, for servers or terminals/clients are allowed provided that:

a) Any device involved in enforcing the copy protection can be verified individually by the method approved described in Section 7.8.2; and

b) The method of copy protection is fully documented and provided to the ITL, who shall test and certify that the protection works as described.

7.6 SYSTEM FAILURE REQUIREMENTS

7.6.1 INTEGRITY PROTECTION.

The TCSS shall be designed to protect the integrity of the pertinent data in the event of a failure. Audit logs, system databases and any other pertinent data shall be stored using reasonable protection methods. For hard disk drives which are used as storage media, data integrity shall be assured in the event of a disk failure. Methods which are acceptable include but are not limited to, multiple hard drives in an acceptable RAID configuration, or mirroring data over two or more hard drives. The method utilized shall also provide open support for backups and restoration. Backup scheme implementation shall occur at least once every day, unless otherwise directed by the CNGC.

7.6.2 RECOVERY.

In the event of a catastrophic failure when the TCSS cannot be restarted in any other way, it shall be possible to reload the database from the last viable backup point and fully recover the contents of that backup. The information shall consist of at least the following:

a) Significant events;

b) Auditing information; and

c) Specific information such as game configuration, security accounts, etc.

7.7 SELF-MONITORING REQUIREMENTS

7.7.1 SELF-MONITORING.

Unless otherwise directed by the CNGC, the TCSS or third party remote access software monitoring tool

shall: implement self-monitoring of all critical interface elements (ex. Central hosts, network devices, firewalls, links to third parties, etc.). The TCSS shall be able to perform this operation with a frequency of at least once in every 24-hour period.

7.8 SOFTWARE VERIFICATION REQUIREMENTS

7.8.1 SOFTWARE VERIFICATION.

The TCSS shall have the ability to allow for an independent integrity check of the software. This shall be accomplished by being authenticated by utilizing a device certified by an ITL, which may be embedded within the TCSS software or have an interface port for a means to utilize an ITL certified device for authentication. The integrity check shall provide a means for verification of the TCSS to identify and validate the programs and files. The ITL shall provide to the CNGC a unique signature for an integrity check within the laboratory certification to be utilized for field verification.

7.8.2 NON-INTERROGATION DEVICES SOFTWARE VERIFICATION.

Program devices which cannot be interrogated may be used provided they are able to be verified by the following methodology:

a) A challenge is sent by the peer device, such as a hashing seed, to which the device shall respond with a checksum of its entire program space using the challenge value.

b) The challenge mechanism and means of loading the software into the device is tested and certified by the ITL and shall be approved by the CNGC.

7.9 SERVER RECALL REQUIREMENTS

7.9.1 SERVER BASED GAME SYSTEM.

The Server that supports a Server Based Game shall be able to provide the following information display:

a) Complete play history for the most recent game played and at least nine (9) games prior to the most recent game for each terminal/client station connected to the Server based game. It shall consist of at least the following:

   i) Game outcome (or representative equivalent),

   ii) Intermediate play steps (ex. Hold and draw sequence, double-down sequence, etc.),

   iii) Credits available,

   iv) Bets placed,

   v) Credits or coins paid, and

   vi) Credits cashed out.

b) A terminal/client which offers games with a variable number of intermediate plays steps per game may satisfy this requirement by providing the capability to display the last 50 play steps;

c) The capability to initiate game recall shall be available at the terminal/client, for recall information specifically associated with the particular terminal/client station initiating the game recall;

d) The capacity to initiate game recall for all terminals/clients that make up the Server Based Gaming System (SBGS) shall be available from the system or server portion of the SBGS;

e) The requirement to display game recall applies to all game programs currently installed on the server portion of the SBGS;

f) The retained transaction history from transactions with a cashless wagering system to include the most recent and the previous thirty-four transaction prior to the most recent transaction for each terminal/client station that incremented any of the cashless in-or out meters; and

g) The capability to initiate transaction history shall be available at the terminal/client for the transaction history specifically associated with the particular terminal/client initiating the history information request.

7.10 DOWNLOADABLE DATA LIBRARY REQUIREMENTS

7.10.1 DATA LIBRARY UPDATE.

The Downloadable Data Library is the formal storage of all certified data files (ex. Game software, peripheral firmware, etc.) that can be downloaded to a terminal/client. The TCSS Downloadable Library shall only be written with secure access which is controlled by the CNGC, in which the vendor/manufacturer/operator will be able to access the Downloadable Data Library provided this access does not permit adding or deleting downloadable data files. The Downloadable Data Library shall only be written using a method that is certified by an ITL and approved by the CNGC.

7.10.2 AUDIT LOG DOWNLOADABLE DATA LIBRARY.

All changes that are made to the Downloadable Data Library, which includes the addition, deletion or changing of game programs, shall be stored in an unalterable audit log, which shall include the following information:

a) Time and Date of the event and/or access;

b) Log In Name; and

c) Downloadable Data files added, deleted or changed.

7.10.3 ACTIVITY LOG DOWNLOADABLE DATA LIBRARY.

Any record of activity between the server and the terminal/client that involves the downloading of program logic, the adjustment of terminal/client settings and/or configurations, or the activation of previously downloaded program logic, shall be stored in an unalterable audit log, which shall include the following:

a) Changes to the terminal/client setting and/or configurations and what those changes were;

b) The terminal/client which the game program was downloaded to, and when applicable the program which it replaced; and

c) The terminal/client which the game program was activated on and the program it replaced.

7.11 TERMINAL/CLIENT DOWNLOAD OF DATA FILES AND CONTROL PROGRAM REQUIREMENTS

7.11.1 CONTROL PROGRAM VERIFICATION.

The terminal/client and/or the applicable server side critical game components shall provide the ability to conduct an independent integrity check of the game program, from a third party outside source. The verification program utilized for the integrity check may be embedded within the game software or have an interface port that is used to authenticate the media with the verification program that shall be read only and not permit the alteration of the program and:

a) Third party verification process shall not include any process or security software provided by the vendor/manufacturer (unless utilized as a secondary verification method).

b) The terminal/client and/or the applicable server side game components shall authenticate all critical files including, but not limited to, executables, data, operating system files, game outcome or operation, or any other files/data/executables, etc. which impacts the credibility and integrity for revenue collection and game play, which reside on the medium.

c) The terminal/client and/or the applicable server side game components shall employ a third party industry standard secure hashing algorithm (ex. MD-5, SHA-1, etc.). If the verification program utilized for the integrity check is embedded, then the vendor/manufacturer shall be prepared to demonstrate the algorithm choice to the ITL and the CNGC.

d) In the event of failed authentication, the terminal/client shall immediately enter an error condition with appropriate audio and/or visual indicator. The error shall require operator intervention.

e) In the event of a failed authentication after the terminal/client has been powered up, the terminal/client shall immediately enter an error condition with the appropriate audio and/or visual indicator. The error shall require operator intervention. The game shall display specific error information and shall not clear until one of the following occurs:

    i) File authenticates properly (following operator intervention);or

    ii) The medium is replaced or corrected: and

        A. The memory is cleared;

        B. The game is restarted; and

        C. Files authenticate correctly.

f) The terminal/client shall verify the game program against the server immediately following the download and prior to allowing the game to become operational for play.

7.11.2 Downloading/Activating Control Program.

When downloading/activating control programs from the TCSS Server to the terminal/client the following requirements shall be met:

a) The terminal/client and/or the TCSS Server shall have a method by which to monitor and report to the monitoring system all external door access during foreground program downloads and/or activation process.
b) When updating the Control Program in a Server Supported Game System (SSGS) configuration, the following methods shall be utilized to store the current game data that is pertinent to the individual terminal/client:

    i) Game data is uploaded and securely stored on the TCSS Server and shall be maintained for a minimum of 24-hours and archived after that time, or maintained in a log or script file. If this method is utilized the process in downloading the new Control Program to the terminal/client shall ensure that all critical areas of memory are overwritten by a default value; or

    ii) Game data is maintained at the terminal/client; or

    iii) If the TCSS is not capable of meeting one of the methods listed, then the proposed alternate method shall be subject to Commissioner Approval and certified by an ITL.

Note: It shall be possible to perform a forensic review of the game which includes viewing the game data at the TCSS Server and/or being able to place it back onto another terminal/client for examination purposes.

c) Prior to execution of updated software, the terminal/client shall be in an idle state with no tilts or credits remaining on the terminal/client for a time frame determined by the Commissioner and the software is successfully authenticated/verified.

7.12 Terminal/Client Configuration Control Requirements

7.12.1 Paytable/Denomination Configuration Changes

Terminal/client Control Programs that offer multiple paytables and/or denominations that can be configured via the TCSS Server shall meet the following requirements:

a) All paytables which are available shall meet the theoretical payback percentage and odds requirements as listed within the ITL certification;

b) The terminal/client and/or TCSS Server maintains the amounts bet and amounts won meters within critical memory for each of the paytables which are available;

c) The terminal/client maintains the Master Accounting meters in dollars and cents or the lowest denomination available.

d) The game is in an idle state with no tilts or credits when the update occurs; and

e) The change shall not cause inaccurate crediting or payment.

7.12.2 Critical Memory Clear Terminal/Client

The process of clearing memory on the terminals/clients via the TCSS shall utilize a secure method that requires Commissioner Approval.

7.12.3 Random Number Generator

In the event the TCSS has the ability to download random values to the terminal/client, the Random Number Generator (RNG) shall function in accordance with the requirements in Section 7.42.

7.13 Terminal/Client Requirements

7.13.1 Physical Security

This section shall meet the requirements of Section 5.2.3 *Patron Safety.*

7.13.2 Safety of Patron

This section shall meet the requirements of Section 5.2.3 *Patron Safety.*

7.13.3 Environmental Effect on Integrity

This section shall meet the requirements of *Section 5.1.1 General Player Interface Requirements.*

7.14 Terminal/Client Hardware Requirements

7.14.1 Hardware Requirements

This section shall meet the requirements of Section 5.2.4 *Microprocessor Controlled.*

7.15 Terminal/Client Cabinet Wiring Requirements

7.15.1 Cabling

This section shall meet the requirements of Section 5.2.5 *Cabinet Wiring.*

7.16 Terminal/Client Identification Requirements

7.16.1 IDENTIFICATION

This section shall meet the requirements of Section 5.2.6 *Player Interface Identification.*

7.17 PLAYER INTERFACE COMMUNICATIONS REQUIREMENTS

7.17.1 PLAYER INTERFACE COMMUNICATIONS

This section shall meet the requirements of Section 5.2.7 *Player Interface Communications.*

7.18 POWER SUPPLY MANIPULATION REQUIREMENTS

7.18.1 POWER SURGE

This section shall meet the requirements of Section 5.2.8 *Power Surges.*

7.19 EXTERNAL DOOR AND COMPARTMENT REQUIREMENTS

7.19.1 EXTERNAL DOOR AND COMPARTMENT

This section shall meet the requirements of Section 5.2.9 *External Doors/Compartment Requirements.*

7.20 LOGIC DOOR AND LOGIC AREA REQUIREMENTS

7.20.1 LOGIC DOOR AND LOGIC AREA

This section shall meet the requirements of Section 5.2.10 *Logic Compartment.*

7.20.2 CRITICAL COMPONENTS

This section shall meet the requirements of Section 5.2.10 *Logic Compartment.*

7.21 FINANCIAL INSTRUMENT COMPARTMENT REQUIREMENTS

7.21.1 FINANCIAL INSTRUMENT COMPARTMENT

This section shall meet the requirements of Section 5.2.11 *Currency Compartments.*

7.21.2 ACCESS TO FINANCIAL INSTRUMENT

This section shall meet the requirements of Section 5.2.11 *Currency Compartments.*

7.22 CRITICAL MEMORY STORAGE REQUIREMENTS

7.22.1 NON-VOLATILE MEMORY

This section shall meet the requirements of Section 5.2.15 *Critical Memory Integrity.*

7.22.2 MEMORY RESET

This section shall meet the requirements of Section 5.2.12 *Function of a Random Access Memory (RAM) Clear.*

7.22.3 Default Reel Position and Display

This section shall meet the requirements of Section 5.2.12 *Function of a Random Access Memory (RAM) Clear.*

7.22.4 Configuration Settings

This section shall meet the requirements of Section 5.2.13 *Configuration Setting.*

7.22.5 Program Storage Media Identification

This section shall meet the requirements of Section 5.2.16 *Program Storage Devices.*

7.23 Contents of Critical Memory Requirements

7.23.1 Terminal/client Critical Memory

This section shall meet the requirements of Section 5.2.14 *Critical Memory Defined.*

7.24 Critical Memory Maintenance Requirements

7.24.1 Critical Memory Storage

The terminal/client and/or TCSS Server shall meet the requirements of Section 5.2.14 *Critical Memory Defined.*

7.24.2 Critical Memory Comprehensive Check

The terminal/client and/or TCSS Server shall meet the requirements of Section 5.2.15 *Critical Memory Integrity.* In addition, upon restart the integrity of all critical memory shall be checked. The critical memory shall be continuously monitored for corruption and comprehensive checks which occur at the start of game play. A redundancy check shall be implemented, and the test methodology shall detect 99.99 percent of all possible failures and enable errors to be identified.

7.24.3 Control Program

This section shall meet the requirements of Section 5.2.19 *Integrity of the Control Program.*

7.24.4 Program Storage Media

This section shall meet the requirements of Section 5.2.19 *Integrity of the Control Program.*

7.25 Unrecoverable Critical Memory Requirements

7.25.1 Unrecoverable Corruption

The terminal/client and/or TCSS Server shall meet the requirements of Section 5.2.15 *Critical Memory Integrity.* In addition, critical memory shall not be cleared automatically and shall result in tilt/error condition which identifies the error and causes the terminal/client to cease further function. The patron's credits shall be displayed to avoid patron disputes. An unrecoverable critical memory error shall require a full memory clear performed by an authorized person.

7.26 PROGRAM STORAGE MEDIA REQUIREMENTS

7.26.1 PROGRAM STORAGE MEDIA

This section shall meet the requirements of Section 5.2.16 *Program Storage Devices.*

7.26.2 EXTERNALLY WRITTEN PROGRAM STORAGE MEDIA

This section shall meet the requirements of Section 5.2.17 *Write Once Program Storage.*

7.26.3 WRITEABLE PROGRAM STORAGE

This section shall meet the requirements of Section 5.2.18 *Writeable Program Storage.*

7.27 PRINTED CIRCUIT BOARD REQUIREMENTS

7.27.1 PRINTED CIRCUIT BOARD IDENTIFICATION

With exception to "off-the-shelf" commercially available printed circuit boards, printed circuit boards designed and manufactured by the vendor/supplier, shall require the following:

a) Each printed circuit board shall be identifiable by some type of name and/or number and revision level;

b) The top assembly revision level of the printed circuit board shall be identifiable (if track cuts and/or patch wires are added to the printed circuit board, then a new revision number or level shall be required to assign to the assembly); and

c) Vendor/Manufacturer/Operator shall ensure that circuit board assemblies used in their terminals/clients conform functionally to the documentation and the certified versions of those printed circuit boards that were evaluated and certified by the ITL.

7.28 SWITCHES AND JUMPERS REQUIREMENTS

7.28.1 SWITCHES AND JUMPERS

If Switches and/or Jumpers are contained within, then the following shall be met:

a) Any switches or jumpers shall be fully documented for certification and evaluation by an ITL.

b) Hardware switches which may alter the Commissioner jurisdictional specific configuration settings, paytables, game denomination, or payout percentages in the operation of the

terminal/client shall meet the required configuration settings in Section 7.2.12 of this document and shall be housed within a logic compartment of the terminal/client. This shall include top award changes (including progressives), selectable Blackjack settings, or any other option that would affect the payout percentage.

7.29 MECHANICAL DISPLAY OF GAME OUTCOMES REQUIREMENTS

7.29.1 MECHANICAL DISPLAY

This section shall meet the requirements of Section 5.2.22 *Mechanical Devices Used for Displaying Game Outcomes.*

7.30 VIDEO MONITOR OR TOUCH REQUIREMENTS

7.30.1 VIDEO MONITOR OR TOUCH SCREEN

This section shall meet the requirements of Section 5.2.23 *Video Monitors/Touch screens.*

7.31 FINANCIAL INSTRUMENT REQUIREMENTS

7.31.1 FINANCIAL INSTRUMENT ACCEPTOR

This section shall meet the requirements of Section 5.2.24 *Bill Acceptors.*

7.31.2 FINANCIAL INSTRUMENT COMMUNICATION

This section shall meet the requirements of Section 5.2.25 *Financial Instrument Communications.*

7.31.3 FACTORY SET FINANCIAL INSTRUMENT VALIDATOR

This section shall meet the requirements of Section 5.2.26 *Factory Set Bill Acceptors.*

7.32 FINANCIAL INSTRUMENT VALIDATOR EVENT REQUIREMENTS

7.32.1 FINANCIAL INSTRUMENT METERING

The terminal/client and/or TCSS Server shall meet the requirements of Section 5.2.28 *Accountability of Bills/Tickets or Other Items Accepted.*

7.32.1 FINANCIAL INSTRUMENT VALIDATOR RECALL

The terminal/client and/or TCSS Server shall meet the requirements of Section 5.2.29 *Bill Acceptor Recall.*

7.33 ACCEPTABLE FINANCIAL INSTRUMENT VALIDATOR LOCATION REQUIREMENTS

7.33.1 FINANCIAL INSTRUMENT VALIDATOR LOCATION

This section shall meet the requirements of Section 5.2.31 *Bill Acceptor Stacker Requirements.*

7.34 FINANCIAL INSTRUMENT VALIDATOR STACKER REQUIREMENTS

7.34.1 FINANCIAL INSTRUMENT VALIDATOR STACKER

This section shall meet the requirements of Section 5.2.30 *Bill Acceptor Error Conditions.*

7.35 REDEMPTION OF CREDIT REQUIREMENTS

7.35.1 CREDIT REDEMPTION

This section shall meet the requirements of Section 5.2.32 *Credit Redemption.*

7.36 FINANCIAL OUTPUT DEVICE (FOD) REQUIREMENTS

7.36.1 PAYMENT BY TICKET/VOUCHER FINANCIAL OUTPUT DEVICES

This section shall meet the requirements of Section 5.2.34 *Payment by Ticket Printers.*

7.36.2 LOCATION OF FINANCIAL OUTPUT DEVICE

This section shall meet the requirements of 5.2.34 *Payment by Ticket Printers.*

7.36.3 FINANCIAL OUTPUT DEVICE ERROR CONDITION.

This section shall meet the requirements of Section 5.2.34 *Payment by Ticket Printers*.

7.37 TICKET/VOUCHER VALIDATION REQUIREMENTS

7.37.1 PAYMENT BY TICKET/VOUCHER FINANCIAL OUTPUT DEVICE.

This section shall meet the requirements of Section 6.3.2 *Ticket Information.*

7.38 TICKET/VOUCHER INFORMATION REQUIREMENTS

7.38.1 TICKET/VOUCHER INFORMATION.

This section shall meet the requirements of Section 6.3.2 *Ticket Information.*

7.39 ISSUANCE AND REDEMPTION OF TICKET/VOUCHER REQUIREMENTS

7.39.1 TICKET/VOUCHER ISSUANCE.

This section shall meet the requirements of Section 6.3.4 *Ticket Issuance*.

7.39.2 ONLINE TICKET/VOUCHER REDEMPTION.

This section shall meet the requirements of Section 6.3.5 *Ticket Redemption.*

7.39.3 OFFLINE TICKET/VOUCHER REDEMPTION.

This section shall meet the requirements of Section 6.3.7 *Offline Ticket Redemption*.

7.40 DISPLAY REQUIREMENTS

7.40.1 RULES OF PLAY.

This section shall meet the requirements of Section 5.1.1 *General Player Interface Requirements* and Section 2.3.3 *General Player Interface Requirements* where applicable.

7.40.2 INFORMATION TO BE DISPLAYED TO PATRON.

This section shall meet the requirements of Section 5.1.1 *General Player Interface Requirements* and Section 2.3.3 *General Player Interface Requirements* where applicable.

7.40.3 MULTI-LINE.

This section shall meet the requirements of Section 5.1.1 *General Player Interface Requirements* and Section 2.3.3 *General Player Interface Requirements* where applicable.

7.41 GAME CYCLE REQUIREMENTS

7.41.1 GAME CYCLE.

This section shall meet the requirements of Section 5.2.44 *Game Cycle.*

7.42 RANDOM NUMBER GENERATOR REQUIREMENTS

7.42.1 SELECTION PROCESS.

This section shall meet the requirements of Section 5.2.45 *RNG Requirements.*

7.42.2 RANDOM NUMBER GENERATOR.

This section shall meet the requirements of Section 5.2.45 *RNG Requirements.*

7.42.3 APPLICABLE TESTING.

This section shall meet the requirements of Section 3.1.5 *RNG Submissions.*

7.42.4 LIVE GAME CORRELATION.

This section shall meet the requirements of Section 5.2.45 *RNG Requirements.*

7.42.5 SCALING ALGORITHMS.

This section shall meet the requirements of Section 5.2.45 *RNG Requirements.*

7.42.6 MECHANICAL BASED RANDOM NUMBER GENERATOR.

All mechanical based Random Number Generator games shall meet the requirements with the exception of Sections 3.1.4, 3.1.5, and 3.1.6 which dictate the requirements for electronic random number generators. Additional mechanical based random number generator games shall meet the following:

a) The mechanical pieces shall be constructed of materials to prevent decomposition of any component over time (ex. A ball shall not disintegrate);

b) The properties of physical items utilized to choose the selection shall not be altered;

c) The patron shall not have the ability to physically interact or come in physical contact or manipulate the machine physically with the mechanical portion of the game; and

d) ITL shall test via PC communication multiple iterations to gather enough data to verify the randomness; additionally, the vendor/manufacturer shall supply live data to assist in the evaluation.

7.42.7 Electronic Card Games.

Electronic card games depicting cards being drawn from a deck shall comply with the following:

a) At the start of each game (hand), the first hand of cards shall be drawn fairly from a randomly shuffled deck; the replacement cards shall not be drawn until needed;

b) Once cards are removed from the deck, they shall not be returned to the deck, except as provided by the rules of the game depicted; and

c) As cards are removed from the deck they shall immediately be used as directed by the Rules of the Game (ex. Cards shall not be discarded due to adaptive behavior by the terminal/client).

7.42.8 Electronic Ball Drawing Games.

a) At the start of each game, only balls applicable to the game shall be depicted. For games with bonus features additional balls that are selected shall be chosen from the original selection without duplicating an already chosen ball;

b) The barrel shall not be re-mixed except as provided by the Rules of the Game depicted; and

c) As balls are drawn from the barrel, they shall immediately be used as directed by the Rules of the Game (ex. Balls shall not be discarded due to adaptive behavior by the terminal/client).

7.43 Percentage Payout Requirements

7.43.1 Payout Percentage.

This section shall meet the requirements of Section 5.2.46 *Software Requirements for Percentage Payout.*

7.43.2 Merchandise Prizes in Lieu of Cash Awards.

This section shall meet the requirements of Section 5.2.48 *Merchandise Prizes in Lieu of Cash Awards.*

7.44 BONUS GAME REQUIREMENTS

7.44.1 BONUS GAMES.

This section shall meet the requirements of Section 5.2.49 *Bonus Games.*

7.44.2 EXTRA CREDITS WAGERED DURING BONUS GAME REQUIREMENTS.

This section shall meet the requirements of Section 5.2.49 *Bonus Games.*

7.45 MYSTERY AWARD REQUIREMENTS

7.45.1 MYSTERY AWARD MINIMUM AND MAXIMUM AMOUNTS.

Upon Commissioner approval, electronic games may offer a Mystery Award (an award that is not specifically called out on the payglass or game screen). However, an electronic game that offers a Mystery Award must indicate the maximum amount the patron could potentially win. If the minimum amount of the potential award is not displayed, it will be assumed to be "0." For those electronic games which offer a mystery award where the method to receive the
award involves strategy or skill, both the minimum and maximum amount of the potential award shall be displayed. This would include methods where the value of the paytable is used in order to make a decision that could increase return to the player (i.e., video poker).

7.46 TERMINAL/CLIENT MULTIPLE GAME REQUIREMENTS

7.46.1 MULTIPLE GAME REQUIREMENTS.

This section shall meet the requirements of Section 5.2.51 *Multiple Games Offered for Play at One Player Interface.*

7.47 ELECTRONIC METERING REQUIREMENTS

7.47.1 CREDIT METER UNITS AND DISPLAY.

This section shall meet the requirements of Section 5.2.36 *Credit Meter.*

7.47.2 CREDIT METER INCREMENTING.

This section shall meet the requirements of Section 5.2.36 *Credit Meter.*

7.47.3 PROGRESSIVE AWARD.

This section shall meet the requirements of Section 5.2.36 *Credit Meter.*

7.47.4 COLLECT METER.

This section shall meet the requirements of Section 5.2.36 *Credit Meter*.

7.47.5 Software Meter Information Access.

Software meter information shall only be accessible by a person authorized by CNGC as set forth in applicable internal control standards and procedures and must have the ability to be displayed on demand using a secure means. Additionally, each TCSS Server and/or terminal/client themselves shall store and maintain the required electronic meters which shall also be displayable at the terminal/client.

7.47.6 Electronic Accounting and Occurrence Meter.

The terminal/client and TCSS Server shall meet the requirements of Section 5.2.37 *Electronic Accounting and Occurrence Meters.*

7.47.7 Required Electronic Meters.

The terminal/client and TCSS Server shall meet the requirements of Section 5.2.37 *Electronic Accounting and Occurrence Meters.*

7.47.8 Multi-Game Specific Meter.

The section shall meet the requirements of Section 5.2.38 *Multi-Game Game Specific Meter.* Additionally, for "double up or gamble" game which is lost, the initial win amount/credits bet amount shall be recorded in the game specific meters.

7.47.9 Double Up or Gamble Meter.

This section shall meet the requirements of Section 5.2.39 *Double Up or Gamble Meter.*

7.48 Communication Protocol Requirements

7.48.1 Communication Protocol.

For each electronic game that is required to communicate with an MCS, the electronic game shall accurately function as indicated by the CNGC approved communication protocol.

7.49 Error Condition Requirements

7.49.1 Error Condition Detection and Display.

This section shall meet the requirements of Section 5.2.41 *Error Conditions.*

7.49.2 Financial Instrument Validator Error.

This section shall meet the requirements of Section 5.2.41 *Error Conditions.*

7.49.3 Financial Output Device Error.

This section shall meet the requirements of Section 5.2.34 *Payment by Ticket Printers.*

7.49.4 DOOR OPEN ERROR.

This section shall meet the requirements of Section 5.2.43 *Door Open Events.*

7.49.5 MISCELLANEOUS ERROR.

This section shall meet the requirements of *Chapter 5 Player Interface and Use Requirements for Authorized Games.*

7.49.6 ERROR CODE.

This section shall meet the requirements of *Chapter 5 Player Interface and Use Requirements for Authorized Games.*

7.50 PROGRAM INTERRUPTION AND RESUMPTION REQUIREMENTS

7.50.1 PROGRAM INTERRUPTION.

This section shall meet the requirements of Section 5.2.42 *Game Interruption and Resumption.*

7.50.2 POWER RESTORATION.

This section shall meet the requirements of Section 5.2.42 *Game Interruption and Resumption.*

7.50.3 SIMULTANEOUS INPUTS.

The program shall not be adversely affected by the simultaneous or sequential activation of various inputs and outputs, such as “play buttons,” which might, whether intentionally or not, cause malfunctions or invalid results.

7.50.4 PROGRAM RESUMPTION.

This section shall meet the requirements of Section 5.2.42 *Game Interruption and Resumption.*

7.50.5 MICROPROCESSOR CONTROLLED REELS.

This section shall meet the requirements of Section 5.2.42 *Game Interruption and Resumption.*

7.51 DOOR OPEN/CLOSE REQUIREMENTS

7.51.1 DOOR METERING.

This section shall meet the requirements of Section 5.2.43 *Door Open Events.*

7.51.2 DOOR OPEN PROCEDURE.

This section shall meet the requirements of Section 5.2.43 *Door Open Events.*

7.51.3 DOOR CLOSE PROCEDURE.

This section shall meet the requirements of Section 5.2.43 *Door Open Events.*

7.52 TAXATION REPORTING LIMIT REQUIREMENTS

7.52.1 TAXATION REPORTING LIMITS.

This section shall meet the requirements of Section 5.2.52 *Taxation Reporting Limits.*

7.53 TEST/DIAGNOSTIC MODE (DEMO MODE) REQUIREMENTS

7.53.1 TEST/DIAGNOSTIC MODE.

This section shall meet the requirements of Section 5.2.53 *Test/Diagnostic Mode (Demo Mode).*

7.53.2 ENTRY OF TEST/DIAGNOSTIC MODE.

This section shall meet the requirements of Section 5.2.53 *Test/Diagnostic Mode (Demo Mode).*

7.53.3 EXITING OF TEST/DIAGNOSTIC MODE.

This section shall meet the requirements of Section 5.2.53 *Test/Diagnostic Mode (Demo Mode).*

7.53.4 TEST GAME.

This section shall meet the requirements of Section 5.2.53 *Test/Diagnostic Mode (Demo Mode).*

7.54 GAME HISTORY RECALL REQUIREMENTS

7.54.1 NUMBER OF LAST PLAYS.

This section shall meet the requirements of Section 5.2.54 *Number Of Last Plays Required.*

7.54.2 LAST PLAY INFORMATION.

This section shall meet the requirements of Section 5.2.54 *Number Of Last Plays Required.*

7.54.3 BONUS ROUND.

This section shall meet the requirements of Section 5.2.54 *Number Of Last Plays Required.*

7.55 SOFTWARE/PROGRAM STORAGE MEDIA VERIFICATION REQUIREMENTS

7.55.1 VERIFICATION.

This section shall meet the requirements of Section 5.2.55 *Software Verification.*

CHAPTER 8

PROGRESSIVE USE AND OPERATION REQUIREMENTS

8.1 GENERAL PROGRESSIVE REQUIREMENTS

8.1.1 GENERAL STATEMENT.

This section reflects additional requirements that, while not specifically required by the Compact, have been determined by the CNGC as being necessary to meet the Tribe's standards for electronic gaming. All electronic games sought to be played in a Choctaw Nation of Oklahoma gaming facility pursuant to the Compact and 25 CFR Part 547 shall meet these additional requirements. It should be noted that all of these standards shall be met "where applicable" (e.g., if the device does not have a mechanical display, adherence to "mechanical display" requirements are not required).

8.1.2 PROGRESSIVE METER/DISPLAY.

A progressive meter/display can be one or more progressive Player Interface(s) that are linked, directly or indirectly, to a display (e.g., mechanical, electrical, or electronic device, including the video display, if applicable) that shows the payoff which increments at a set rate of progression as credits are wagered. For games that have progressives such as "mystery jackpot," the payoff does not have to be displayed to the patron, although there shall be an indication as to this type of feature on the game. The following requirements apply to all progressive meter displays:

a) A progressive meter shall be visible to all Patrons who are playing a device, which may potentially win the progressive amount if the progressive jackpot combination appears, except for "mystery jackpots."

b) A patron shall have notice that he is playing a progressive game and not have to play the max bet amount to find out. The above are parameters that are verified on-site prior to implementation.

c) The progressive meter shall display the current total of the progressive jackpot in the monetary value or credits (the monetary value may vary for multi-site progressive displays.) Because the polling cycle does cause a delay, the jackpot meter need not precisely show the actual monies in the progressive pool at each instance.

d) The use of odometer and other "paced" updating displays are allowed. The progressive meter shall display the winning value within 30 seconds of the jackpot being recognized by the central system. In the case of the use of paced updating displays, the system jackpot meter shall display the winning value after the jackpot broadcast is received from the central system.

    i) The actual amount won on a jackpot shall never be less than the amount shown on the progressive meter display.

e) If the progressive meter(s) progresses to its maximum display amount, the meter shall freeze and remain at the maximum value until awarded to a patron. This can be avoided by setting the jackpot

limit in accordance with the digital limitations of the sign.

f) When multiple items of information are to be displayed on a Player Interface or progressive meter, it is sufficient to have the information displayed in an alternating fashion.

g) When a progressive jackpot is recorded on an electronic Player Interface, which is attached to the progressive controller, the progressive controller shall allow for the following to occur on the device and/or progressive display:

   i) Display of the winning amount;

   ii) Display of the electronic Player Interface identification that caused the progressive meter to activate if more than one (1) electronic Player Interface is attached to the controller; and

   iii) The progressive controller shall reset and display the reset value, including any accumulated escrow amount and continue normal play.

NOTE: Any device that has a feature that doubles, or triples, etc., any win shall have a sign that states the progressive award will not be doubled or tripled if won during the feature, if this is the intention.

h) For progressives offering multiple levels of awards, the patron must always be paid the higher progressive amount, if a particular combination is won that should trigger the higher paying award. This may occur when a winning combination may be evaluated as more than one of the available paytable combinations. (For example, a straight flush is a form of a flush and a royal flush is a form of a straight flush.) Therefore, there may be situations where the progressive levels shall be exchanged to ensure the patron is being awarded the highest possible progressive value based on all combinations the outcome may be defined as.

8.1.3 PROGRESSIVE CONTROLLERS.

The requirements of this section are intended to apply equally to one progressive Player Interface linked to a progressive controller or is internally controlled, as well as several progressive Player Interfaces linked to one progressive controller within one casino or multiple casinos. A progressive controller is all of the hardware and software that controls all communications among the devices that calculates the values of the progressives and displays the information within a progressive Player Interface link (if applicable – progressive Player Interface(s) may be internally controlled) and the associated progressive meter. This equipment includes but is not limited to PC-based computers, wiring, and collection nodes, etc. The method by which system jackpot parameter values are modified or entered is to be secure. Progressive controllers shall:

a) During the "normal mode" of progressive Player Interfaces, the progressive controller shall continuously monitor each device on the link for credits bet and shall multiply the same by the rate of progression and denomination in order to determine the correct amounts to apply to the progressive jackpot. This shall be at least 99.99% accurate.

b) The progressive controller or other approved progressive system component shall keep the following information in non-volatile memory:

i) The number of progressive jackpots won on each progressive level if the progressive display has more than one winning amount;

ii) The cumulative amounts paid on each progressive level if the progressive display has more than one winning amount;

iii) The maximum amount of the progressive payout for each level displayed;

iv) The minimum amount of the progressive payout for each level displayed; and

v) The rate of progression for each level displayed.

Progressive controller shall have the ability to display this information on demand. Additionally, progressive meters shall be 99.99% accurate.

c) When a controller error occurs, it is preferred that it alternates the displays, or equivalent, between the current amount and an appropriate error message that is visible to all patrons, or can alert the operator to the error condition. The game that is using the progressive is to be disabled, and an error shall be displayed on the progressive meter, other approved progressive system component or Player Interface if any of the following events occur:

i) During a communication failure;

ii) When there have been multiple communication errors;

iii) When a controller checksum or signature has failure;

iv) When a controller's RAM or PSD (program storage device) mismatch or failure occurs; or

v) When the jackpot configuration is lost or is not set.

d) The progressive controller shall have a secure means of transferring a progressive jackpot and/or prizes to another progressive controller or other approved progressive system component. Transferring of progressive jackpots must meet the CNGC's Tribal Internal Control Standards.

e) There shall be a secure, two-way communication protocol between the main game processor board and progressive. In addition, the progressive system shall be able to:

i) Send to the electronic Player Interface the amount that was won for metering purposes; and

ii) Constantly update the progressive display as play on the link is continued.

f) Each progressive controller used with progressive Player Interfaces shall be housed in a secure environment allowing only authorized accessibility. Access to the controller must conform to the CNGC's Tribal Internal Control Standards.

g) All progressive Player Interfaces or any approved progressive system component shall display, upon request, the following information for each progressive prize offered (where applicable):

i) CURRENT VALUE: current prize amount;

ii) OVERFLOW: amount exceeding limit;

iii) HITS: number of times this progressive was won;

iv) WINS: total value of wins for this progressive or a history of the last 25 progressive hits;

v) BASE: starting value (the initial amount of a progressive jackpot shall begin at or above an award for that particular Player Interface that makes the entire meter payout greater than the minimum percentage requirement, if one is set);

vi) LIMIT: jackpot limit value (if the jackpot is capped at a maximum limit, this standard does not require that the overflow amounts be added to the next starting value);

vii) INCREMENT: percentage increment rate;

viii) SECONDARY INCREMENT: percentage increment rate after limit is reached;

ix) HIDDEN INCREMENT: percentage increment rate for the reserve pool (the next base amount shall be computed or posted to advise the Patron of this contribution);

x) RESET VALUE: the amount the progressive resets to after the progressive is won; and

xi) The participating Player Interfaces.

8.1.4 LINKED PLAYER INTERFACE ODDS.

Each device on the link shall have the same probability of winning the progressive, adjusted for the value of the wager. For the purpose of this requirement, “same” is defined as odds not exceeding a 5% difference and the payout percentage not exceeding a 1% difference. For instance, the probability shall remain the same for multiple denomination games based on the monetary value of the wager (e.g., A two (2) coin $1 game has the probability of one (1) in 10,000 and a two (2) coin, $2 game on the same link has the probability one (1) in 5,000.)

8.2 MULTI-SITE PROGRESSIVE REQUIREMENTS

8.2.1 MULTI-SITE PROGRESSIVES.

Multi-site progressive Player Interfaces are interconnected in more than one casino. The purpose of a multi-site progressive system is to offer a common progressive jackpot (system jackpot) at all participating locations. Multi-site progressive systems shall meet the following requirements:

a) Be certified in two phases:

i) Initial laboratory testing, where the ITL will test the integrity of the Player Interface(s) in conjunction with a progressive system in the laboratory setting with the equipment assembled; and

ii) On-site certification, where the progressive communications and set up are tested on the casino floor prior to implementation.

b) It is recommended that the method of communication be a non-shared, dedicated line or equivalent. Dial-tone systems may be used as long as devices at the local site would not be able to be disabled from another outside line or manipulated by any other means. When the method of communication is a shared line, appropriate encryption and security must be in place to avoid corruption or compromise of data.

c) Multi-site systems shall ensure that security information and the amounts wagered information is communicated, at least once every 60 seconds for terrestrial lines (dedicated phone lines), and a reasonable amount of time for radio frequency, from each participating device to the central computer system.

d) All multi-site property systems shall utilize an encryption method that has been approved by the ITL. Such encryption method shall include the use of different encryption "keys" or "seeds" so that encryption can be changed in a real-time fashion.

e) The on-line provision is to be able to monitor the meter readings and error events of each device regardless of any outside monitoring system. Therefore, the on-line security system requirement when Player Interfaces are in play is not altered in any way.

f) The central computer site shall be equipped with non-interruptible power supply that will allow the central computer to conduct an orderly shutdown if the power is lost. Should the system utilize hard disk peripherals, the central computer shall be capable of on-line data redundancy.

g) A Player Interface shall immediately disable itself and suspend play if communication is lost to the local collection unit and security hub. The Player Interface may resume play only when communication to the local hub is restored. If the communication is lost between the local hub and the central computer, the Player Interface may continue to play. However, once communications are reestablished, the system wide totals are to be updated; not withstanding this rule if the communication is lost for more than 24 hours and the site must be shut down.

h) Any "multi-site" system shall supply, upon request, the following reports:

i) PROGRESSIVE SUMMARY: A report indicating the amount of, and basis for, the current jackpot amount (the amount currently in play);

ii) AGGREGATE REPORT: A report indicating the balancing of the system with regard to system wide totals; and

iii) PAYOFF REPORT: A report that will clearly demonstrate the method of arriving at the payoff amount. This will include the credits contributed beginning at the polling cycle,

immediately following the previous jackpot and will include all credits contributed up to and including the polling cycle which includes the jackpot signal.

NOTE: Credits contributed to the system after the jackpot occurs in real time, but during the same polling cycle, shall be deemed to have been contributed to the progressive amount prior to the jackpot. Credits contributed to the system subsequent to the jackpot message being received, as well as credits contributed to the system before the jackpot message is received by the system, but registered after the jackpot message is received at the system, will be deemed to have been contributed to the progressive amount of the next jackpot, if applicable.

i) All meter reading data shall be obtained in real time in an on-line, automated fashion. For progressive amount reconciliation purposes, the progressive system shall return the "credits bet" meter readings on all Player Interfaces attached to the system. The meter readings shall be identical to the meter information retained in the Player Interface(s) accounting meters.

j) The multi-site progressive system shall have the ability to monitor entry into the front door of the Player Interface and report it to the central system immediately.

k) If a jackpot is recognized in the middle of a system-wide poll cycle, the overhead display may contain a value less than the aggregated jackpot amount calculated by the central system. The credit values from the remaining portion of the poll cycle will be received by the central system but not the local site, in which case the jackpot amount paid will always be the higher of the two reporting amounts; and

l) When multiple jackpots occur, where there is no definitive way of knowing which jackpot occurred first, they will be deemed to have occurred simultaneously; and therefore, the gaming regulator shall adopt procedures for payment of such jackpot occurrences. In addition, if there is a communication failure, a winning patron wagering at a non-updated site may also be eligible to a jackpot amount.

CHAPTER 9

CASHLESS SYSTEMS

9.1 GENERAL REQUIREMENTS

9.1.1 INTRODUCTION.

One or more electronic accounting systems shall be required to perform reporting and other functions in support of the authorized electronic games. These systems may communicate with other computers, Player Interfaces and game components utilizing these standards and procedures, as set forth in the Compact. The electronic accounting system shall not interfere with the outcome of any electronic game functions.

9.1.2 GENERAL CASHLESS TRANSACTION REQUIREMENTS.

The following standards shall be met in connection with any cashless transaction system:

a) All patron account information must be stored on at least two (2) separate nonvolatile media;

b) An audit file must be kept of all financial transactions against the account. This file must be stored in at least two (2) separate nonvolatile media, and be accessible for purposes of audit and disputes resolution to authorized individuals. This file must be available on-line for a minimum of thirty (30) days, after which it must be available off-line for a minimum of one hundred eighty (180) days;

c) Access controls must be in place to guarantee that unauthorized individuals will not have access to account information or history;

d) Passwords or personal identification numbers (PINs), if used, must be protected from unauthorized access;

e) All means for communicating information within the system shall conform to these Uniform Standards;

f) Patron accounts shall follow accounting procedures that are designed to verify and protect the accurate recording of all patron transactions;

g) Any card or other tangible instrument issued to a patron for the purpose of using the cashless transaction system shall bear on its face a control or inventory number unique to that instrument;

h) Encoded bearer instruments (printed or magnetic) may include coupons and other items distributed or sold for game play, promotional, advertising or other purposes, but may not include cash. Such instruments must be in electronically readable form in addition to having unique identification information printed on the instrument face. The daily and monthly reporting must include with respect to such instruments:

    i) Cash converted to game play credits;

ii) Outstanding unredeemed balance;

iii) Game play credits converted to cash;

iv) Game play credits used; and

v) Game play credits won

i) All customer accounts or instruments must have a redemption period of at least fourteen (14) days;

j) No ATM card, financial institution debit card or credit card shall be used as part of any cashless transaction system; and

k) Any "smart card" system that is part of the cashless transaction system shall be tested by the ITL and approved by the CNGC to ensure the integrity of patron funds.

i) Any smart card must store on the card or on the system using the card an audit trail of the last ten (10) transactions involving the use of the card. Each transaction record must include, at a minimum, the type of transaction, the amount of the transaction, the date of the transaction, the time of the transaction, and the identification of the Player Interface or cashier Interface or other points of cash exchange where the transaction occurred. The minimum daily and monthly reporting for smart card activity must include:

A. Total of cash transferred to smart cards;

B. Total of smart card amounts transferred to cash;

C. Total of smart card amounts transferred to game play credits;

D. Total of game play credits transferred to smart card amounts; and

E. Total unredeemed smart card balance.

ii) Systems shall allow patron tracking, maintenance tracking, and other gaming management or marketing functions. These systems shall not interfere with, or in any way effect, the outcome of any game being played. Systems shall be permissible that allow progressive prize management with the certification of an ITL approved by the CNGC.

9.2 ADDITIONAL REQUIREMENTS

9.2.1 GENERAL STATEMENT.

A cashless system may be entirely integrated into an On-Line Monitoring System (MCS) or exist as an entirely separate entity. Cashless systems may include promotional, bonusing, or patron account based systems.

9.2.2 ERROR CONDITIONS.

The following sections outline the error conditions that apply to the cashless system, which must be monitored, and a message must be displayed to the patron at the host card reader for the following:

a) Invalid PIN or Patron ID (can prompt for re-entry up to maximum allowed); and

b) Account Unknown.

9.2.3 TRANSFER OF TRANSACTIONS.

If a patron initiates a cashless transaction and that transaction would exceed game configured limits (i.e., the credit limit), then this transaction shall be processed in the following manner:

a) The maximum limit permitted by the game shall be the amount transferred, and

b) To avoid patron disputes, the patron shall be clearly notified he has transferred less than the amount requested.

9.2.4 SECURITY REQUIREMENTS.

The communication process used by the Player Interface and the host system must be robust and stable enough to secure each cashless transaction such that failure event(s) can be identified and logged for subsequent audit and reconciliation. In addition, cashless systems must conform to the following Security Requirements.

a) The number of users that have the requisite permission levels/login to adjust critical parameters are limited.

b) Only a logged-in, authorized employee shall have the ability to access all patron information. Security of this information (including patron PIN codes or equivalent patron identification) must be maintained at all times.

c) Any adjustment to an account balance would require a supervisor's approval with all changes being logged and/or reported indicating who, what, when, and the item value before and after the change, with the reason.

9.2.5 PREVENTION OF UNAUTHORIZED TRANSACTIONS.

The following minimal controls shall be implemented by the host system to ensure that games are prevented from responding to commands for crediting outside of properly authorized cashless transactions (hacking):

a) The network hubs are secured (either in a locked/monitored room or area) and no access is allowed on any node without valid login and password;

b) The number of stations where critical cashless applications or associated databases could be accessed is limited; and

c) Procedures shall be in place on the system to identify and flag suspect patron and employee

accounts to prevent their unauthorized use to include:

i) Having a maximum number of incorrect PIN entries before account lockout;

ii) Flagging of "hot" accounts where cards have been stolen;

iii) Invalidating accounts and transferring balances into a new account; and

iv) Establishing limits for maximum cashless activity in and out as a global or individual variable to preclude money laundering.

9.2.6 Diagnostic Tests on a Cashless Player Interface.

Controls must be in place for any diagnostic functionality available at the device such that all activity must be reported to the system that would reflect the specific account(s) and the individual(s) tasked to perform these diagnostics. This would allow all cashless diagnostic activity that affects the Player Interface's associated electronic meters to be audited by the CNGC.

9.2.7 Transaction Auditing.

The central system shall have the ability to produce logs for all pending and completed cashless transactions. These logs shall be capable of being filtered by:

a) Machine number;

b) Patron account; and

c) Time/date.

9.2.8 Financial and Patron Reports.

The system shall have the ability to produce the following financial and patron reports:

a) Patron Account Summary and Detail Reports. These reports shall be immediately available to a patron upon request. These reports shall include beginning and ending account balance, transaction information depicting Player Interface number, amount, and date/time.

b) Liability Report. This report is to include previous days starting value of outstanding cashless liability, aggregate cashless-in and out totals, and ending cashless liability.

c) Cashless Meter Reconciliation Summary and Detail Reports. These reports will reconcile each participating Player Interface's cashless meter(s) against the host system's cashless activity.

d) Cashier Summary and Detail Reports. These reports will include patron account, buy-ins and cash-out, amount of transaction, date and time of transaction.

9.2.9 Account Balance.

Current account balance information should be available on demand from any participating Player Interface via the associated card reader (or equivalent) after confirmation of patron identity and be presented, in terms of currency, to the patron.

CHAPTER 10

REDEMPTION TERMINAL/KIOSK STANDARDS

10.1 INTRODUCTION

10.1.1 GENERAL STANDARDS STATEMENT.

Redemption kiosks shall meet all provisions of these Standards, including the memory and communication requirements. In addition, kiosks are required to have an interface to the validation system. Regardless of the method of interfacing with the system, the redemption kiosk must use a communication protocol and must not write directly to the system database. The redemption kiosk must only process the payment based on commands from the system .

10.2 KIOSK HARDWARE REQUIREMENTS

10.2.1 CABINET SECURITY.

The main door shall be manufactured of materials that are suitable for allowing only legitimate access to the inside of the cabinet. Doors and associated hinges shall be capable of withstanding unauthorized efforts to gain access to the inside of the kiosk, and shall leave evidence of tampering if an unauthorized entry is made.

10.2.2 CABINET WIRING.

Kiosk shall be designed so that any power and data cables into and out of the kiosk can be routed so that they are not accessible to the general public. Wires and cables that are routed into a logic area shall be securely fastened within the interior of the kiosk.

10.2.3 ON/OFF SWITCH.

On/off switches which control electrical current shall be located in a place which is readily accessible within the interior of the kiosk so that power cannot be disconnected from outside of the kiosk utilizing the on/off switch. On/off positions of the switch shall be clearly labeled.

10.2.4 SWITCHES AND JUMPERS.

Switches and/or jumpers contained within a Kiosk shall be fully documented for evaluation by the ITL.

10.2.5 IDENTIFICATION.

The Kiosk shall have an identification label affixed to both the inside and the outside of the cabinet, which shall not be easily removable without leaving evidence of tampering. The affixed label shall contain the following information:

a) Manufacturer’s name;

b) Unique serial number;

c) Kiosk model number; and

d) Date of manufacture.

10.2.6 PATRON SAFETY.

Electrical and mechanical parts and design principals of the electronic associated hardware shall not subject a patron to any physical hazards. All documentation for UL, CSA, EC, EMC, AS3100, etc. or equivalent certifications and any other certification required by statute, regulation, law or Act shall be provided to the ITL.

10.2.7 INTEGRITY.

The ITL shall perform tests to determine whether or not outside influences affect performance to the patron or create cheating opportunities. A kiosk shall be able to withstand the following tests and resume operation without operator intervention:

a) Electro-magnetic Interference: Kiosk shall not create electronic noise which affects the integrity or fairness of the neighboring associated equipment;

b) Electro-static Interference: Protection against static discharges requires that the hardware be grounded in such a way that static discharge energy shall not permanently damage or permanently inhibit the normal operation of the electronics or other components. The kiosk may exhibit temporary disruption, however the kiosk shall exhibit the capacity to recover and complete any interrupted function without loss or corruption of any control or data information associated with the system when subjected to an electro-static discharge greater than human body discharge up to 27kV;

c) Radio Frequency Interference (RFI): Kiosks shall not be adversely affected by radio frequency interference. The manufacturer shall supply to the ITL documentation showing the Kiosk has had Radio Frequency Interference testing against a recognized standard and has passed; and

d) Magnetic Interference: Kiosks shall not be adversely affected by magnetic interference. The manufacturer shall supply to the ITL documentation showing the Kiosk has had Magnetic Interference testing against a recognized standard and has passed.

NOTE: Commercial components which are affected (ex. PC monitor, etc.) shall provide a method to determine the state the Kiosk was in if any of the components fail from static discharge.

10.2.8 PATRON INTERFACE COMMUNICATION.

Patron Interface Communications (PIC) shall provide a method of notification when: any Error Condition occurs or the “Call Attendant” or other service request is initiated by the patron. A PIC may include, but is not limited to, a tower light, an audible alarm or a message displayed on the Player Interface.

10.2.9 EXTERNAL DOOR/COMPARTMENT.

The interior of the kiosk shall not be accessible when all doors are closed and locked. Doors shall be manufactured of materials which are suitable for allowing only legitimate access to the inside of the cabinet. The kiosk doors shall be capable of withstanding unauthorized efforts to gain access to the inside of the kiosk, and shall leave evidence of tampering if an unauthorized entry is made.

10.2.10 LOGIC DOOR AND/OR LOGIC AREA.

The kiosk shall utilize a logic area which shall be a locked area within the cabinet which houses electronic components that have the potential to significantly influence the operation of the kiosk. There may be more than one logic area within a kiosk. The following components are required to be housed within in a logic area:

a) Communication controller electronics and components housing the communication program storage media or the communication board for the on-line system;

b) All flash memory devices that affect the kiosk function;

c) CPU's and other electronic components involved in the operation of the kiosk; and

d) Electronics and components housing display program storage media.

10.2.11 CURRENCY COMPARTMENTS.

Currency compartments shall be locked separately from the main cabinet area. The kiosk shall be fitted with sensors that indicate door open/close or stacker removed.

10.2.12 VIDEO MONITORS/TOUCH SCREENS.

All video monitors and/or touch screens shall meet the following:

a) A touch screen shall be accurate and once calibrated shall maintain that accuracy for at least the manufacturers recommended maintenance period;

b) A touch screen shall be able to be re-calibrated by authorized individuals possessing a valid gaming license without access to the cabinet other than opening the main door; and

c) There shall be no hidden or undocumented buttons/touch points anywhere on the screen.

10.2.13 BACK-UP OF MEMORY.

The kiosk shall utilize battery back-up, or an equivalent that is capable of maintaining the accuracy of all critical memory for thirty (30) days after power is discontinued from the kiosk.

10.3 FINANCIAL ACCEPTOR REQUIREMENTS

10.3.1 FINANCIAL INSTRUMENT ACCEPTOR.

All financial instrument acceptors shall be able to detect the entry of valid bills, coupons, paper, token or

other CNGC approved notes, and provide a method to enable the kiosk software to interpret and act appropriately upon a valid or invalid input. All financial instrument acceptors shall be electronically based and be configured to ensure that they only accept financial instruments of legal tender. The financial instrument input system shall be constructed in a manner that protects against vandalism, abuse or fraudulent activity. Additionally, credits shall only be registered when:

a) The financial instrument has passed the point where it is accepted and stacked; and

b) The financial instrument acceptor has sent the "irrevocable stacked" message (or equivalent message) to the kiosk.

10.3.2 COMMUNICATION.

All financial instrument acceptors shall communicate to the kiosk utilizing a bi-directional protocol.

10.3.3 FACTORY SET FINANCIAL INSTRUMENT ACCEPTORS.

If financial instrument acceptors are designed to be factory set only, it shall not be possible to access or conduct maintenance or adjustment to those financial instrument acceptors in the field, other than the following:

a) The selections of financial instruments or other CNGC approved notes and their limits;

b) Changing of certified control program media or downloading of certified software;

c) Adjustment of the tolerance level for accepting financial instruments of varying quality shall not be allowed externally to the kiosk. . This can be accomplished through lock and key, physical switch settings or other CNGC approved methods.

d) Maintenance, adjustment and repair per approved factory procedures; or

e) Options that set the direction or orientation of acceptance.

10.3.4 FINANCIAL INSTRUMENT ACCEPTOR REQUIREMENTS.

All financial instrument acceptors shall not be adversely affected by the following:

a) Electro-static discharge;

b) Power surges;

c) Radio frequency interference;

d) Electro-magnetic interference;

e) Environmental extremes;

f) Interconnecting cables from financial instrument acceptor devices to the kiosk shall not be exposed

external to the kiosk; and

g) The manufacturer shall supply documentation for the financial instrument acceptors for the above tests performed to a recognized standard as approved by the CNGC .

10.3.5 Financial Instrument Acceptor Stacker.

Each financial instrument acceptor shall have a secure stacker and all accepted financial instruments shall be deposited into the secure stacker. The secure stacker shall be attached to the kiosk in such a manner so that it cannot be easily removed by unauthorized means and shall meet the following additional requirements:

a) The financial instrument acceptor shall have a stacker full sensor;

b) There shall be a separate key access to the stacker area. The key shall be separate from the main door. In addition, a separate key shall be required to remove the financial instruments from the stacker; and

c) A message indicating that the stacker door has been accessed shall be recorded.

10.3.6 Self-Test.

The financial instrument acceptor shall perform a self-test at each power up. In the event of a self-test failure the financial instrument acceptor shall automatically disable itself (ex. Bill reject state) until the error state has been cleared which requires operator intervention.

10.4 Software Requirements

10.4.1 Critical Memory.

Critical memory which stores data which is considered vital to the continued operation of the kiosk includes the following:

a) All electronic meters;

b) Ticket Voucher Redeemed Log; and

c) The last normal state the kiosk software was in prior to interruption.

10.4.2 Non-Volatile Memory Reset.

Following the initiation of a Non-Volatile Memory reset procedure the program shall execute a routine which initializes critical bits in non-volatile memory to the default state. All memory locations intended to be cleared as per the non-volatile memory clear process shall be fully reset in all cases. For kiosks that allow for partial non-volatile memory clears, the methodology in doing so shall be accurate.

10.4.3 Critical Memory Maintenance.

Critical memory storage shall be maintained by a method that enables errors to be identified and corrected. This method may involve signatures, checksums, partial checksums, multiple copies, timestamps and/or effective use of validity codes.

NOTE: If hard drive file storage of critical memory is utilized the critical data shall be maintained accurately. The ITL shall review and test the method used.

10.4.4 Data Alteration.

The kiosk shall not permit the alteration of any meter or error condition log information without supervised access controls. In the event meter or error condition log data is changed, an audit log shall be capable of being produced to document the following:

a) Data element altered;

b) Data element value prior to alteration;

c) Data element value after alteration;

d) Time and Date of alteration; and

e) Personnel that performed alteration.

10.5 Communication Requirements

10.5.1 Communication Components.

For Ticket/Voucher or Coupon Issuance and/or Redemption features, the kiosk shall be designed to allow for communication with a Validation System. All communication between kiosks and the Validation System shall be secured. This network security shall be implemented by the CNGC.

10.6 Error Condition Requirements

10.6.1 Error Conditions.

Error conditions shall initiate a PIC and shall be recorded. The kiosk shall be able to recover to the state it was in immediately prior to the interruption occurring, including during payment. The kiosk shall be capable of detecting and displaying the following error conditions:

a) Currency out error (require attendant/operator intervention);

b) System and kiosk not communicating;

c) Power loss or power reset;

d) Cash Dispenser empty or timed out (require attendant/operator intervention);

e) Non Volatile Memory error (require attendant/operator intervention);

f) Low Non Volatile Memory battery (require attendant/operator intervention);

g) Ticket/Voucher-in jam (require attendant/operator intervention);

h) Door open;

i) Financial instrument acceptor stack full;

j) Financial instrument acceptor door open;

k) Stacker door open or stacker removed; and

l) Financial output device errors, which shall include:

    i) Out of paper/paper low;

    ii) Financial output device jam/failure; and

    iii) Financial output device disconnected.

NOTE: If the kiosk uses error codes instead of a text explanation of the error conditions, a description of error codes and their meanings shall be affixed on the inside of the Kiosk.

NOTE: If any of the above error conditions occur during the acceptance and/or escrowing of a ticket voucher, the kiosk shall return the ticket voucher to the patron without a status change on the Validation System. If the error condition is cleared, the kiosk shall process the ticket voucher and have a status of "Redeemed "on the Validation System.

10.7 PROGRAM INTERRUPTION & RESUMPTION REQUIREMENTS

10.7.1 PROGRAM INTERRUPTION.

When the kiosk's main door is opened, the kiosk shall cease activity, enter an error condition, and display an appropriate error message, disable financial instrument acceptance, and initiate a PIC. Following any program interruption, the software shall be able to recover to the state it was in immediately prior to the interruption occurring.

10.7.2 PROGRAM RESUMPTION.

The kiosk shall return to its original state and perform the following procedures:

a) Kiosk control programs shall test themselves for possible corruption due to failure of the program storage media. The authentication shall utilize the Cyclic Redundancy Check (CRC) calculations at least 16-bit. Any other authentication method shall require CNGC approval and be tested by an ITL;

b) Any communication to an external device shall not begin until the program resumption routine, including self-tests, is completed successfully; and

c) The integrity of all critical memory shall be checked.

10.8 TRANSACTION LIMIT REQUIREMENTS

10.8.1 TRANSACTION LIMITS.

Each kiosk shall have the ability to have transaction limits for ticket/voucher issuance and also ticket/voucher redemption. The configuration of the transaction limit shall be via a secure method as approved by the CNGC. The CNGC shall approve the transaction limit.

10.9 METERING REQUIREMENTS

10.9.1 METER STORAGE.

Electronic metering information shall be maintained in critical memory at the kiosk and shall be accessible only by an authorized person possessing a valid gaming license.

10.9.2 ACCOUNTING METERS.

Electronic accounting meters shall be at least eight (8) digits in length. If the meter is being used in dollars and cents, at least eight (8) digits shall be used for the dollar amount. The meter shall roll over to zero upon the next occurrence, any time the meter is eight (8) digits or higher and after 99,999,999 has been reached or any other value approved by the CNGC. The following accounting information shall be maintained with critical memory:

a) A “handpay” meter shall reflect the cumulative amounts paid by an attendant in the event that a ticket/voucher cannot be printed;

b) A “total in” meter that accumulates the total value of all financial instruments accepted by the kiosk. Separate In meters shall report the value of all tickets/vouchers redeemed and the value of all currency redeemed; and

c) A “total out” meter for payment issued by the kiosk. Separate Out meters shall report the value of all financial instruments dispensed by the kiosk.

10.10 VERIFICATION REQUIREMENTS

10.10.1 INTEGRITY CHECK.

The kiosk shall have the ability to allow for an independent integrity check of the software from an outside source. This shall be accomplished by being authenticated by utilizing a device certified by an ITL, which may be embedded within the kiosk software or have an interface port for a means to utilize an ITL certified device for authentication. The integrity check shall provide a means for verification of the kiosk system to identify and validate the programs and files. The ITL shall provide to the CNGC a unique signature for an integrity check within the laboratory certification to be utilized for field verification.

10.11 TICKET/VOUCHER FINANCIAL OUTPUT DEVICE REQUIREMENTS

10.11.1 TICKET/VOUCHER PRINTED INFORMATION.

A ticket/voucher produced by a kiosk shall contain the following printed information:

a) Gaming facility name/Site identifier;

b) Kiosk identification information;

c) Date and time (24 hour format);

d) Alpha and numeric dollar amount of the ticket/voucher;

e) Ticket sequence number;

f) Validation number;

g) Bar code;

h) Type of transaction or other method for differentiating ticket/voucher types; and

i) Date and time ticket/voucher shall expire.

NOTE: Additionally, the CNGC approved system used to validate the payout ticket/voucher , the ticket/voucher information on the central system shall be retained at least as long as the ticket is valid at that gaming facility location.

10.11.2 FINANCIAL OUTPUT DEVICE LOCATION.

The financial output device shall be located within a locked area of the kiosk, but not within the logic area or the drop box.

CHAPTER 11

WIRELESS DEVICE REQUIREMENTS

11.1 WIRELESS DEVICES

11.1.1 GENERAL STATEMENT.

Wireless Devices refer to any devices which communicate wirelessly over a local area network or have an impact on a wireless network. This includes, but is not limited to:

a) A Wireless Access Point (WAP) is a device that allows wireless devices to connect to a wired network using Wi-Fi, Bluetooth or other wireless protocols.

b) A Wireless Connectivity Device (WCD) is a device that provides the interface through which a wireless network can be accessed by other hardware within the gaming establishment (e.g., a wireless network adaptor on a PC).

c) A Wireless Client Device is a device that converts communications from the Wireless Gaming System into a human interpretable form, and converts human decisions into communication format understood by the Wireless Gaming System.

NOTE: It is recommended that all Wireless Devices are Underwriter's Laboratory (or equivalent) approved for device safety, resistance to power surges, electrostatic discharge, magnetic interference, and extreme environmental conditions.

11.1.2 CONFIGURATION.

All Wireless Devices shall be configured as follows:

a) All network management functions must:

   i. Authenticate all users on the network; and

   ii. Encrypt all network management communications.

b) All software that will be communicating over the wireless network shall implement user access control with strong authentication. Any administrative access shall require an additional level of control.

c) If any authentication credentials are hard coded on a component of the wireless network, they shall be encrypted.

d) Communication on the secure network shall only be possible between approved wireless components that have been registered and authenticated as valid on the network. No unauthorized communications to components and/or access points shall be allowed.

e) Any component that uses the wireless network to communicate shall meet all of the encryption and authentication requirements set forth within this standard.

11.2 WIRELESS ACCESS POINTS (WAP)

11.2.1 GENERAL STATEMENT.

a) The Wireless Access Point (WAP) relays data between the wireless device(s) and the rest of the network. All devices that provide one or more WAPs shall:

b) Be installed in a secure, controlled, or inaccessible area to allow for the restriction of physical access to the device.

c) Be constructed in such a way as to be resistant to physical damage to the hardware or corruption of the contained firmware/software by normal usage.

d) Have all physical connection ports secured to prevent unauthorized access to the network via physically connecting to the Wireless Access Point. All unused ports/connections shall be physically blocked, or software disabled.

e) Limit wireless network coverage to an approved area. (For example, directional antennae, geo fencing, etc.)

NOTE: It is recommended that all WAPs are certified by the Wi-Fi Alliance ®.

11.2.2 CONFIGURATION.

All WAP Devices shall be configured as follows:

a) The default administration login and password shall be changed from the factory default to a secure value.

b) The default network password shall be changed from the factory default to a secure value.

c) The “Service Set Identifier (SSID)” for the device shall be configured as follows:

   i. The value shall be changed from the factory default to a secure value.

   ii. The SSID shall not contain any reference to the site name, manufacturer, or any other reference that could be easily discerned.

d) Access to the administrative functions of the Wireless Access Point device shall be restricted to connections from the wired side of the network utilizing a secure protocol with a privileged user account.

NOTE: Alternate network management methods and protocols will be examined on a case by case basis.

11.3 WIRELESS CONNECTIVITY DEVICES (WCD)

11.3.1 GENERAL STATEMENT.

All Wireless Connectivity Devices (WCDs) shall have the capability of being configured to meet the configuration requirements set forth in the "Configuration" section of this document above.

NOTE It is recommended that all WCDs are certified by the Wi-Fi Alliance ®.

11.4 WIRELESS CLIENT DEVICES

11.4.1 GENERAL STATEMENT.

A Wireless Client Device allows for the connection to, and interaction with a Wireless Gaming System. All hardware devices that allow for the use of Wireless Client software shall be compatible with or incorporate a WCD.

NOTE: In some cases, a Wireless Client Device may be a patron-owned device, while in other instances, it can be an operator-supplied device that is controlled by the licensed operator of the WGS and checked out for use by a registered patron. A patron-owned device may interact with the WGS through a client app that is downloaded and installed onto the device, or alternately, the device can simply connect to a secure site hosting the WGS through a browser interface.

11.4.2 OTHER REQUIREMENTS.

All proprietary hardware devices developed to support wireless gaming shall meet the applicable CNGC standards for its intended use, as well as the requirements set forth in this document.

11.5 WIRELESS GAMING SYSTEMS DEVICES

11.5.1 GENERAL STATEMENT.

Any system components that utilize wireless communication to communicate with the gaming network shall meet the following requirements:

a) Be compatible with or incorporate a WCD.

b) Be located in a secure and controlled location within the gaming facility such that access to

the system devices is limited to authorized personnel.

11.6 OTHER WIRELESS DEVICES

11.6.1 GENERAL STATEMENT.

Wireless peripherals including, but not limited to, keyboards, mice, presenters/pointers, headphones, and mobile devices (e.g., patron phones or tablets) shall be used in accordance with the following security controls:

a) These devices shall not be used to communicate sensitive data, as defined elsewhere in this standard, unless they conform to all wireless communication security and encryption requirements outlined in this document.

b) All operations of these components shall be used in accordance with the applicable requirements of this technical standard, and other applicable CNGC technical standards.

11.7 SOFTWARE REQUIREMENTS FOR WIRELESS COMPONENTS

11.7.1 WIRELESS DEVICES – SOFTWARE REQUIREMENTS.

11.7.2 IDENTIFICATION.

Wireless Client Device software shall contain sufficient information to identify the software and revision level of the information stored on the device, which may be displayed via a display screen.

NOTE: The process used in the identification of the software and revision level will be evaluated on a case-by-case basis.

NOTE: For patron-owned devices that rely upon a downloadable app, the device can support a menu option or "app manager" to provide identification information for the app, including a program ID / program name and version number. If a browser interface is used instead, the software running on the accessed site can be identified in a similar manner.

11.7.3 INDEPENDENT CONTROL PROGRAM VERIFICATION.

It must be possible to allow for an independent integrity check of the device's software from an outside source. This is required for all software that may affect the integrity of the system. This shall be accomplished by being authenticated by a third-party device, or by allowing for removal of the media such that it can be verified externally. Other methods shall be evaluated on a case-by-case basis by the CNGC. This integrity check will provide a means for field verification of the software to identify and validate the program.

NOTE: For patron-owned devices, there is no intention to verify or signature the client software on the device itself. However, a copy of the "official app" that resides in an app store, and which is the official published version for installation, can be verified and its signature confirmed as legitimate. Alternately, if a browser interface is used, the software running on the site can be verified.

11.7.4 VALIDATION.

Software utilized in a wireless network shall have the ability to authenticate that all software being utilized is valid and upon failure of the authentication routines, cease all gaming operations, and display an error message until corrected. This authentication shall take place upon installation of the software, each time the software is loaded for use, upon the initiation of an active session, and upon request by an authorized user account.

NOTE: Program verification mechanisms will be evaluated on a case-by-case basis and approved by the CNGC based on industry-standard security practices.

11.8 WIRELESS CLIENT - SOFTWARE

11.8.1 GENERAL STATEMENT.

Wireless Client software is any software downloaded to, or installed on a device which is used to interface with an associated system. Wireless Operator Client devices are for display and interface functions only. All credits, meters, critical data, and program logic shall be implemented and performed by the associated system. All Wireless Client software shall conform to the requirements listed above in "Wireless Devices – Software Requirements" section of this document as well as those listed below within this section (11.8).

11.8.2 CLIENT-SERVER INTERACTIONS.

The following requirements apply to Wireless Client Device software and the client-server interactions, as applicable:

a) The Wireless Client Software must not automatically alter any client-specified firewall rules to open ports that are blocked by either a hardware or software firewall;

b) The Wireless Client Software must not access any ports (either automatically or by prompting the user to manually access) which are not necessary for the communication between the client and the server;

c) If the Wireless Client software includes additional non-game or non-administrative related functionality, this additional functionality shall not alter the software's integrity in any way.

d) The Wireless Client Software shall not possess the ability to override the volume settings of the Wireless Client Device
.

e) It is recommended that auto complete, password caching, or other methods that will fill in the password field are disabled for Wireless Client Software.

NOTE: For patron-owned devices, the above Client-Server Interaction requirements can apply and ensure that whatever client software is downloaded does not arbitrarily change or modify settings on the patron-owned device without the acknowledgement and/or consent of the patron upon installation/download. Alternately, accessing a site through a browser interface shall not alter patron-owned device settings without the consent of the patron.

11.8.3 LIMITED AREA OF OPERATION.

Connection to, and use of a Wireless Network for gaming or administration purposes shall be limited to a specific location as defined by the CNGC. Once the device is removed from the defined area, it shall immediately disable and cease all gaming or administration operations.

11.8.4 COMPATIBILITY VERIFICATION.

During any installation or initialization and prior to establishing a session, the Client Software used in conjunction with the System shall detect any incompatibilities or resource limitation with the device on which it is installed that would prevent proper operation of the Wireless Client software. If any incompatibilities or resource limitations are detected the client and system shall:

a) Notify the user of any incompatibility and/or resource limitation preventing operation(e.g., software version, minimum specifications not met, etc..); and

b) Prevent any gaming or administrative activity while the incompatibility or resource limitation exists.

11.8.5 CONTENT.

Wireless Client Software shall not contain any functionality deemed to be malicious in nature by the regulatory body. This includes, but is not limited to, unauthorized file extractions/transfers, unauthorized player device modifications, unauthorized access to any device stored personal information(contacts, calendar, etc..), and malware.

11.8.6 COOKIES.

All application level cookies used shall contain no malicious code.

11.8.7 COMMUNICATIONS.

Communications between the Wireless Client and associated system shall take place over a secure network connection that meets all of the requirements set forth in this standard.

11.8.8 USER INTERFACE REQUIREMENTS.

The user interface is defined as an application or program through which the operator views and/or interacts with the client software to communicate their actions to the associated system. The User Interface shall meet the following:

a) Any resizing or overlay of the User Interface shall be mapped accurately to reflect the revised display, buttons, or touch/click points.

b) The functions of all buttons, touch or click points represented on the user interface shall be clearly indicated within the area of the button, or touch/click point and/or within the help menu. There shall be no functionality available through any buttons or touch/click points that are hidden or undocumented on the client device.

c) The display of the instructions and information shall be adapted to the user interface. For example, where the player client device uses technologies with a smaller display screen, it is permissible to present an abridged version of the game information accessible directly from within the game and make available the full/complete version of the game information via another method, such as a secondary screen, help menu, or other interface that is easily identified on the visual game screen.

11.8.9 SIMULTANEOUS INPUTS.

The program shall not be adversely affected by the simultaneous or sequential activation of the various inputs and outputs which might, whether intentionally or not, cause malfunctions or invalid results.

11.9 WIRELESS OPERATOR CLIENT - SOFTWARE

11.9.1 GENERAL STATEMENT.

Wireless Operator Client software is utilized by Gaming Venue personnel to perform administrative tasks within the property (e.g., Ticket Validation, Status monitoring, etc.…). All Wireless Operator Client software shall conform to the requirements listed in “Wireless Client – Software” section of this document as well as those listed below within this section (11.9).

11.9.2 REQUIRED FUNCTIONABLILTY FOR WIRELESS OPERATOR CLIENT SOFTWARE.
In addition to the applicable

CNGC requirements for the connected system, the Wireless Operator Client software shall meet the following:

a) All available options presented in the Wireless Operator Client shall be tied to the account of the

operator logged in. Only access available to the logged in account shall be available through the Wireless Operator Client.

b) Wireless Operator Client devices shall not store sensitive data or system information.

11.9.3 OPERATOR SESSIONS.

An operator session is defined as a time frame during which an operator or other Gaming Venue personnel can utilize a Wireless Operator Client device to perform administrative functions on the gaming floor on a wireless device.

a) A Wireless Operator session is initiated by the operator logging in to their controlled account using their secure username and password via either their own device, or a device supplied by the operator/property.

b) An operator shall be provided with (or have created) an electronic identifier such as a digital certificate or an account description and a password that will be utilized to start a session.

c) Operator account security shall be established according to the applicable CNGC system standards.

11.9.4 OPERATOR SESSION INACTIVITY.

The wireless operator client software shall employ a mechanism that detects session inactivity and terminates a session when applicable.

a) If the Wireless Operator Client device does not receive input from the operator within 5 minutes, or other period of time as defined by the regulator, the session shall time out and require reactivation. Gaming Venue personnel can re-establish their session by re-establishing their login with the system. This process shall include, at a minimum, the manual entry of the operators secure password or other accepted methods.

b) No further operator functionality is permitted until a new session is established.

11.10 WIRELESS PLAYER CLIENT - SOFTWARE

11.10.1 GENERAL STATEMENT.

Wireless Player Client software is utilized by a player to take part in any gaming activity over a wireless network. All Wireless Player Client software shall conform to the requirements listed in “Wireless Client – Software” section of this document as well as those listed immediately below within this section (11.10).

11.10.2 REQUIRED FUNCTIONABILITY FOR WIRELESS PLAYER CLIENT SOFTWARE.

In addition to the applicable CNGC requirements for Server Based Gaming System Clients defined in Chapter 7, "Terminal/Client Server System Standards", the Wireless Player Client software shall meet the following:

a) Wireless Player Client devices shall not contain any logic utilized to generate the result of any game. All critical functions including the generation of any game (and the return to the player) shall be generated by the Gaming System and be independent of the Wireless Player Client.

b) Wireless Player Client devices shall not be capable of conducting gaming activity if disconnected from the associated gaming server.

c) Wireless Player Client devices shall not store sensitive data or system information.

d) Wireless Player Client software shall not be able to transfer data to other Wireless Client software other than chat functions (e.g., text, voice, video, etc.…) and approved files (e.g. user profile pictures, photos, etc.…).

e) Game outcome shall not be affected by the effective bandwidth, link utilization, bit error rate or other characteristic of the communications channel between the Gaming System and the Player Client.

11.10.3 WIRELESS GAMING SESSIONS.

A wireless gaming session is defined as a time frame during which a player can participate in gaming activity. A wireless gaming session can be established by one of the following methods:

a) **Operator-Supplied Device**. The player may obtain a wireless client device from the WGS operator after completing the necessary process defined within the CNGC WGS internal controls.

b) **Player Owned Device**. The player may obtain/download an application or software package containing the wireless player client software, or access the client application via a browser interface.

   i. The client software installation process shall include a validation process that requires system validation of the installation and links an end user connection to a specific account for the duration of the session.

   ii. Where cookies are used, the player must be informed of their usage upon installation. When cookies are required for game play, game play cannot occur if the Wireless Player Client Device does not accept them.

11.10.4 PLAYER SESSION MANAGEMENT.

A player session is managed by one of the following methods:

a) Established Player Account. The player shall log in to the gaming system using their established player account.

   i. Player accounts shall conform to CNGC WGS internal controls, and the requirements defined in the CNGC's rules and regulations for player accounts. In absence of specific regulations, CNGC Chapter 5, "Cashless Wagering System Standards", shall be applied.

   ii. The player may wager the credits that are currently present in their account during this gaming session. Credits can be added and redeemed from their personal account via the standard methods of deposits and withdrawals from a player account.

b) Guest Play. The Gaming Venue personnel will initialize the client software on the device and establish a connection to the gaming system using a secure method.

   i. Credits can be added to the wireless gaming session and these credits will be available for play using the client device. The player may increase their available credits via this same process.

   ii. The player may redeem the credit balance on the wireless gaming session by returning to the origination point of the session or via Gaming Venue personnel, who will pay them the credit balance as per the standard methods of withdrawal.

NOTE: Alternate implementations of player session handling will be reviewed on a case by case basis.

11.10.5 WIRELESS GAMING SESSION INACTIVITY.

The wireless player client software shall employ a mechanism that detects session inactivity and terminates a wireless gaming session when applicable.

a) If the Wireless Player Client device does not receive input from the player within 15 minutes, or other period of time as defined by CNGC, the wireless gaming session shall time out and require reactivation.

b) If such a termination occurs, the Wireless Player Client device shall display to the player that the session has timed out and inform them of the steps needed to be taken to reestablish the gaming session.

   i. For gaming sessions tied to player accounts, the player may establish a new session and resume play by re-establishing their login with the system. This process shall include, at a minimum, the manual entry of the player's secure password.

ii. For all other gaming sessions, the device must be returned to the origination point of the session or property representative for reactivation.

c) No further game play is permitted until a new wireless gaming session is reestablished.

d) Should a timeout due to user inactivity occur during a game cycle, the current game will be treated as an incomplete game.

11.10.6 PLAYER FACING HISTORY.

A 'replay last game' facility must be provided, either as a re-enactment or by description. The replay must clearly indicate that it is a replay of the entire previous game cycle, and must provide the following information (at a minimum):

a) The date and time the game started and/or ended;

b) The display associated with the final outcome of the game, either graphically or via a clear text message;

c) Total player cash / credits at start and/or end of play;

d) Total amount bet;

e) Total cash / credits won for the prize (including Progressive Jackpots);

f) The results of any player choices involved in the game outcome;

g) Results of any intermediate game phases, such as gambles or feature games; and

h) Amount of any promotional awards received (if applicable).

11.11 **WIRELESS GAMING SYSTEM - SOFTWARE**

11.11.1 REQUIRED FUNCTIONALITY.

a) The Wireless Gaming System shall meet all applicable CNGC requirements for Server Based Game Systems, as defined in Section 7.9.1.

b) The Wireless Gaming System shall incorporate a location tracking component that can track the locations of all wireless client devices logged on to the system and detect when any devices have been transported out of the allowed area. When client devices are discovered to be out of the allowed area, the system shall disable any current gaming or operator sessions associated with those devices.

11.11.2 GAME ENABLE/DISABLE.

The following requirements apply to the disabling and re-enabling of gambling on the Wireless Gaming System:

a) The Wireless Gaming System must be able to disable or enable all gambling on command;

b) The Wireless Gaming System must be able to disable or enable individual games on command;

c) The Wireless Gaming System must be able to disable or enable individual gaming sessions on command; and

d) When any gambling is disabled or enabled on the Wireless Gaming System an entry must be made in an audit log that includes the reason for any disable or enable.

11.11.3 CURRENT GAME.

When a game or gaming activity is disabled:

a) The game is not to be accessible to a player once the player's game has fully concluded.

b) The player should be permitted to conclude the game in play (i.e., bonus rounds, double up/gamble and other game features related to the initial game wager should be fully concluded).

c) If wagers have been placed on pending real-life events:

    i. The game screens must clearly define what happens to the wagers if the gaming activity is to remain disabled and the corresponding real-life event is completed, and the Wireless Gaming System must be capable of returning all bets to the players, or settling all bets, as appropriate.

    ii. The game screens must clearly define what happens to the wagers if the gaming activity is to re-enable before the corresponding real-life event is completed, and the Wireless Gaming System must be capable of returning all bets to the players, or leaving all bets active, as appropriate.

11.11.4 INCOMPLETE GAMES.

A game is incomplete when the game outcome remains unresolved, or the outcome cannot be properly seen by the player. Incomplete games may result from:

a) Loss of communications between the Wireless Player Client and the gaming system;

b) A system restart;

c) A Wireless Player Client restart or malfunction;

d) Abnormal termination of the Client Software; or

e) A game-disable command by the system during play.

11.11.5 COMPLETION OF INCOMPLETE GAMES.

The Wireless Gaming System may provide a mechanism for a player to complete an incomplete game. An incomplete game shall be resolved before a player is permitted to participate in another instance of the same game.

a) If the player has an incomplete game, the Wireless Gaming System is to present the incomplete game for completion upon reconnection or whenever a new player session is established.

    i. Where no player input is required to complete the game, the game shall display the final outcome as determined by the Wireless Gaming System and game rules, and the player`s account shall be updated accordingly.

    ii. For single-player, multi-stage games, where player input is required to complete the game, the game shall return the player to the game state immediately prior to the interruption and allow the player to complete the game; and
    (Note: The addition of an optional bonus or feature, such as double-up or gamble, would not make a game multi-stage.)

    iii. For multi-player games, the game shall display the final outcome as determined according to the game rules and/or terms and conditions, and the player`s account shall be updated accordingly.

b) Wagers associated with an incomplete game that can be continued shall be held by the Wireless Gaming System until the game completes. Player accounts shall reflect any funds held in incomplete games.

11.11.6 CANCELLATION OF INCOMPLETE GAMES.

Wagers associated with an incomplete game that can be continued, but remaining undecided for a time period to be specified by the regulatory body can be voided and the wagers forfeited or returned to the player provided that:

a) The game rules and/or the terms and conditions shall clearly define how wagers will be handled when they remain undecided beyond the specified time period and the Wireless Gaming System

shall be capable of returning or forfeiting the wagers, as appropriate.

b) In the event that a game cannot be continued due to a Wireless Gaming System action, all wagers shall be returned to the players of that game.

11.11.7 SHUTDOWN AND RECOVERY.

The Wireless Gaming System shall have the following shutdown and recovery capabilities:

a) The Wireless Gaming System shall be able to perform a graceful shut down with no loss of data, and only allow automatic restart on power up after the following procedures have been performed as a minimum requirement:

i. Program resumption routine(s), including self-tests, complete successfully;

ii. All critical control program components of the Wireless Gaming System have been authenticated using an approved method (ex. CRC, MD5, SHA-1, etc.); and

iii. Communications with all components necessary for Wireless Gaming System operation have been established and similarly authenticated.

b) The Wireless Gaming System shall be able to identify and properly handle the situation where master resets have occurred on other gaming components which affect game outcome, win amount or reporting.

c) The Wireless Gaming System shall have the ability to restore the system from the last backup.

d) The Wireless Gaming System shall be able to recover all critical information from the time of the last backup to the point in time at which the Wireless Gaming System failure or reset occurred.

11.11.8 MALFUNCTION.

The Wireless Gaming System shall:

a) Not be affected by the malfunction of Wireless Player Client Devices other than to institute the incomplete games procedures in accordance with these requirements; and

b) Include a mechanism to void bets and pays in the event of a malfunction of the Wireless Gaming System itself if a full recovery is not possible.

11.11.9 BACK-END HISTORY.

For each individual game played, the following information, in addition to the above required elements

within the “Player Facing History” section is to be recorded, maintained and easily demonstrable, per session, by the Wireless Gaming System for a period as defined in Section 11.10.6.:

a) Unique player ID;

b) Contributions to Progressive Jackpot pools (if applicable);

c) Game status (in progress, complete, etc.);

d) The table number (if applicable) at which the game was played;

e) The paytable used; and

f) Game identifier and version.

11.12 GAME REQUIREMENTS

11.12.1 General Statement.

All game software to be used in conjunction with the wireless gaming system shall meet the requirements outlined within CNGC Chapter 1, “Electronic Game Standards”, to ensure player fairness.

11.12.2 PEER TO PEER (P2P).

P2P game rooms are those environments which offer players the opportunity to gamble with and against each other. In these environments, the operator usually does not engage in the gambling event as a party (e.g., house banked gaming), but usually provides the gambling service or environment for use by its players, and takes a rake, fee, or percentage for the service. Systems that offer P2P games shall do the following, unless otherwise specified, in addition to the above applicable game rules:

a) Provide a mechanism to reasonably detect and prevent player collusion, artificial player software, unfair advantages, and ability to influence the outcome of a game or tournament;

b) Provide warnings about how bots can affect play, so that players can make an informed decision whether to participate and provide steps to report suspected player-bot usage;

c) Prevent authorized players from occupying more than one seat at any individual table;

d) Provide authorized players with the option to join a table where all authorized players have been selected at random;

e) Inform authorized players of the length of time each player has been seated at a particular table;

f) Clearly indicate to all authorized players at the table whether any players are playing with house

money (shills) or are proposition players; and

g) Must not employ artificial player software to act as an authorized player, except in free play or training modes.

11.12.3 COMPUTERIZED PLAYERS.

The following requirements apply to use of computerized players in free play or training modes:

a) The software may employ the use of Artificial Intelligence (AI) in order to facilitate game play for demo, free games, or training modes.

b) The use of AI software must be clearly explained in the help menus.

c) All computerized players must be clearly marked at the tables so that players are aware of which players are not human.

11.12.4 CONTESTS/TOURNAMENTS.

An organized event that permits a player to either purchase or be awarded the opportunity to engage in competitive play against other players may be permitted providing the following rules are met.

a) While enabled for tournament play, the tournament feature shall not accept real money from any source, nor pay out real money in any way, but shall utilize tournament specific credits, points or chips which shall have no cash value.

b) Wireless gaming contest/tournament rules are available to a registered player on the client application through which the contest/tournament is being conducted. The rules must include at a minimum:

i. All conditions registered players must meet to qualify for entry into, and advancement through, the contest/tournament.

ii. Any conditions concerning late arrivals or complete tournament no-shows and how auto- blind posting and/or initial entry purchase is handled.

iii. Specific information pertaining to any single contest/tournament, including the amount of money placed in the prize pool.

iv. The distribution of funds based on specific outcomes.

v. The name of the organization (or persons) that conducted the contest/tournament on behalf of, or in conjunction with, the operator if applicable.

c) The results of each contest/tournament shall be made available on the wireless gaming client software for the participants to review. Subsequent to being posted, the results of each contest/tournament are available upon request from the gaming establishment. The recording includes the following:

i. Name of the event;

ii. Date(s) of event;

iii. Total number of entries;

iv. Amount of entry fees;

v. Total prize pool; and

vi. Amount paid for each winning category.

Note: For free contests/tournaments (i.e., registered player does not pay an entry fee), the information required by the above must be recorded except for the number of entries, amount of entry fees and total prize pool.

11.13 **RANDOM NUMBER GENERATOR (RNG) REQUIREMENTS**

11.13.1 GENERAL STATEMENT.

The random number generator to be used in conjunction with the wireless gaming system must be cryptographically strong at the time of submission and meet the randomness requirements established by the CNGC and as stated within Chapter 1, “Electronic Game Standards”, for RNG requirements.

11.14 TAXATION

11.14.1 GENERAL STATEMENT.

The Wireless Gaming System must support a mechanism that is capable of identifying all wins that are subject to taxation and providing the necessary information in accordance with CNGC taxation requirements as defined in Chapter 1, “Electronic Game Standards”, Section 5.2.52 entitled ‘Taxation Reporting Limits’.

11.15 WIRELESS NETWORK SECURITY REQUIREMENTS

11.15.1 WIRELESS AUTHENTICATION AND ENCRYPTION REQUIREMENTS.

11.15.2 GENERAL STATEMENT.

This section defines the encryption and authentication requirements for a wireless network being utilized to communicate gaming data. The CNGC requires the use of strong user authentication, authorization, and encryption.

a) All WLAN solutions shall provide for multi-factor authentication at the network and device level. NOTE: The CNGC will consider secure encryption and authentication methodologies on a case by case basis.

b) If the router supports WPA2 authentication, it shall be enabled as follows:

    i. All Access Points shall be configured with Enterprise Mode enabled or with a strong pre- shared key.
    ii. All Access points shall be IEEE 802.11 compliant.

c) A password or other secure method shall be enabled for each client that connects to the network.

d) A fallback method for failed wireless authentication (e.g., forgotten passwords) shall be at least as strong as the primary method.

e) Advance Encryption Standards (AES) or equivalent with a minimum of 256 bit encryption shall be used to support integrity and confidentiality services.

f) The Pairwise Master Key (PMK) utilized shall have a lifetime of 24 hours or less. Alternatively, it is acceptable for the PMK be changed during pre-scheduled maintenance downtime as described in an internal control document.

g) The Group Master Key (GMK) utilized shall have a lifetime of 8 hours or less.

11.15.3 WIRED EQUIVALENT PRIVACY (WEP).

WEP shall not be used.

Note: If it is not possible for the manufacturer to implement WPA2 protocol, the CNGC will consider the implementation of WEP as a secure encryption and authentication on a case by case basis.

11.16 WIRELESS COMMUNICATION PROTOCOL

11.16.1 GENERAL.

The wireless communication link between the wireless client/terminal, access point, secure gateway/mobility controller and the secure authentication wireless gaming server shall function as indicated by the CNGC-approved communication protocol implemented. To ensure the integrity of the Wireless Gaming System (WGS) for data communicated, confidentiality, and for encrypting the data communicated, any communication between the server(s) and the mobile client/terminal shall use appropriate

authentication and cryptographic protocols to provide mutual authentication of the mobile unit (client/terminal) and the server. The WGS design and implementation shall comply with Institute of Electrical and Electronic Engineers (IEEE) 802.11, and/or other relevant industry-accepted wireless security standard, Establishing Wireless Robust Security Networks, in conjunction with other applicable security conscience components, these items will ultimately make up the WGS. Any alternative measures shall require CNGC approval.

11.16.2 SENSITIVE DATA.

Communication of sensitive data must be secure from eavesdropping, access, tampering, intrusion or unauthorized alteration. Sensitive data includes, but is not limited to:

a) RNG seeds and outcomes;

b) Encryption keys, where the implementation chosen requires transmission of keys;

c) PINs/Passwords;

d) Transfers of funds;

e) Player tracking information;

f) Download Packages; and

g) Any information that affects game outcome.

11.16.3 COMMUNICATION PROTOCOL(S).

Each device shall be reviewed on a case-by-case basis by the network operators and the CNGC.

a) Each component of a wireless network that communicates gaming data shall utilize a communications protocol with encryption and authentication.

b) Each component of a wireless network shall function in accordance with its implemented communications protocol.

c) Unsecured devices may not be used for any function that affects game play, player account management, or any other critical gaming function.

11.16.4 WIRELESS DEVICE COMMUNICATION WITH OTHER SYSTEMS.

In the event that components of the wireless portion of the network are utilized in conjunction with other

traditional wired systems; (i.e., On-Line Monitoring and Control Systems, Ticket Validation Systems, Progressive Systems, etc.), the communications between the wireless device and the traditional network shall meet the following:

a) All communications shall pass through at least one approved application-level firewall, and provide an alternate network path unless the alternate route conforms to the requirements of this document and has independent security (i.e., keys are not the same as other networks), and

b) All communications shall be performed utilizing the network authentication and security methods outlined in this standard.

11.16.5 WIRELESS NETWORK SOFTWARE SECURITY.

A wireless network shall:

a) Implement a security method that links the clients and/or devices to the server, such that the software may only be used by authorized clients and/or devices.

b) Implement a security scheme that utilizes metamorphic security keys. In general, if keys or seeds are used, they shall not be hard coded, and shall change automatically, over time, as a function of the communication link. Each method shall be reviewed by the network operators and the CNGC on a case-by-case basis.

c) Perform mutual authentication to ensure that clients only communicate with valid networks.

d) Validate clients and devices at pre-defined time intervals with at least one method of authentication as described above. This time interval shall be configurable based on network operator requirements;

e) Close active sessions if user authentication has exceeded the number of failed attempts. The number of failed attempts shall be configurable based on network operator requirements;

f) Provide a printable report of failed network access attempts, including the:

   i. time and date stamp,

   ii. the device name, and

   iii. the hardware identifier of all devices requesting access to the network.

11.16.6 WIRELESS NETWORK AUTHENTICATION METHODS.

Communications between devices on the wireless network shall use protocols designed for securing,

authenticating and encrypting wireless networks. One of the following encrypted tunneling protocols shall be utilized to secure communication of all gaming- related data over the wireless network:

a) Protected Extensible Authentication Protocol (Protected EAP or PEAP),

b) Extensible Authentication Protocol- Transport Layer Security (EAP-TLS),

c) Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS),

d) Virtual Private Network with L2TP/IPsec (VPN),

e) Point to Point Tunneling Protocol (PPTP), or

f) Secure Sockets Layer (SSL).

Note: These methods are authenticated against LDAP, RADIUS, Kerberos or Microsoft Active Directory servers, as well as local databases stored on the secure gateway controller. The implementation of any other methods will be reviewed on a case by case basis.

Note: Authentication schemes using Public Key Infrastructure shall require certificate validation, ideally, in both directions (e.g., client certificates).

Note: Alternate authentication and encryption methods will be evaluated on a case by case basis.

11.16.7 COMPONENT FAILURES.

The wireless network shall have sufficient redundancy and modularity to accommodate a component failure to prevent the interruption of the wireless operations. There shall be redundant copies of each audit log and system database, where applicable, on the wireless server with open support for backups and restoration. This includes a wireless network that has support for failover redundancy. A backup scheme implementation shall occur in compliance with the Disaster Recovery Policy, although all methods will be reviewed on a case-by-case basis by the CNGC.

11.16.8 Recovery Requirements.

In the event of a catastrophic failure when the wireless network cannot be restarted in any other way, it shall be possible to reload the system from the last viable backup point and fully recover the contents of that backup. Backups shall consist of at least the following minimum information, as applicable:

a) Significant events,

b) Auditing information, and

c) Specific site information such as unique configuration settings, security accounts, etc.

11.16.9 USER AUTHORIZATION REQUIREMENTS.

The Wireless Gaming System shall implement the following user authorization requirements:

a) Wireless Gaming Systems shall employ a secure and controlled mechanism that is capable of verifying that the wireless device is being operated by an authorized person.

b) The mechanism shall be able to be initiated on demand and on a regular basis.

c) Any authorization information communicated by the wireless device to the system for identification purposes must be obtained at the time of the request from the Wireless Gaming System and not be stored on the wireless client device.

NOTE: Stationary devices that cannot be moved by the patron may be exempted from these requirements on a case by case basis.

11.16.10 CONNECTIVITY.

The Wireless Gaming System shall provide methods to:

a) Enroll and un-enroll system components;

b) Enable and disable specific system components;

c) Ensure that only enrolled and enabled system components participate in the wireless gaming system; and

d) Ensure that the default condition for all components shall be un-enrolled and disabled.

11.17 INFORMATION SYSTEM SECURITY (ISS) REQUIREMENTS

11.17.1 GENERAL STATEMENT.

To ensure players are not exposed to unnecessary security risks, these security requirements will apply to the following critical components of the Wireless Gaming System:

a) Wireless Gaming System components which record, store, process, share, transmit or retrieve sensitive player information, e.g., transaction details, authentication information, player account balances;

b) Wireless Gaming System components which generate, transmit, or process random numbers used to determine the outcome of games or virtual events;

c) Wireless Gaming System components which store results or the current state of a player's wager;

d) Points of entry to and exit from the above systems (other systems which are able to communicate directly with core critical systems); and

e) Wireless networks which transmit sensitive player information.

11.18 Information Security Policy

11.18.1 GENERAL STATEMENT.

An information security policy document shall be in effect to describe the operator's approach to managing information security and its implementation. The information security policy shall:

a) Have a provision requiring review when changes occur to the Wireless Gaming System or the operator's processes which alter the risk profile of the Wireless Gaming System;

b) Be approved by management;

c) Be communicated to all employees and relevant external parties;

d) Undergo review at planned intervals; and

e) Delineate the responsibilities of the operator's staff and the staff of any third parties for the operation, service and maintenance of the Wireless Gaming System and/or its components.

11.19 ADMINISTRATIVE CONTROLS

11.19.1 HUMAN RESOURCE SECURITY.

The security roles and responsibilities of employees should be defined and documented in accordance with the information security policy.

a) All employees of the organization shall receive appropriate security awareness training and regular updates in organizational policies and procedures as needed for their job function.

b) An access control policy shall be established, documented, and reviewed based on business and security requirements for physical and logical access to the Wireless Gaming System and / or its components.

c) Employees shall only be provided with access to the services or facilities that they have been specifically authorized to use.

d) Management shall review users' access rights at regular intervals using a formal process.

e) The access rights of all employees to the Wireless Gaming System and / or its components shall be removed upon termination of their employment, contract, or agreement, or adjusted upon change.

11.19.2 THIRD PARTY SERVICES.

The security roles and responsibilities of third party service providers should be defined and documented in accordance with the information security policy.

a) Agreements with third party service providers involving accessing, processing, communicating or managing the Wireless Gaming System and / or its components, or adding products or services to the Wireless Gaming System and / or its components shall cover all relevant security requirements.

b) The services, reports and records provided by the third party shall be monitored and reviewed by management at least once a year.

c) Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

d) The access rights of third party service providers to the Wireless Gaming System and / or its components shall be removed upon termination of their contract or agreement, or adjusted upon change.

11.19.3 ASSET MANAGEMENT.

All assets housing, processing or communicating controlled information, including those comprising the operating environment of the Wireless Gaming System and/or its components, should be accounted for and have a nominated owner in accordance with the information security policy.

a) An inventory shall be drawn up and maintained of all assets holding controlled items.

b) Assets shall be classified in terms of their criticality, sensitivity, and value.

c) Each asset shall have a designated “owner” responsible for ensuring that information and assets are appropriately classified and defining and periodically reviewing access restrictions and classifications.

d) A policy shall be included on the acceptable use of assets associated with the Wireless Gaming System and its operating environment.

e) A procedure shall exist for removing assets from service and adding new assets.

f) De-commissioned equipment shall have storage media removed and disposed of securely using documented procedures.

g) Removable storage media should be disposed of securely when no longer required, using documented procedures.

11.19.4 ENCRYPTION KEY MANAGEMENT.

The management of encryption keys shall follow defined processes in accordance with the information security policy.

a) There shall be a documented process for obtaining or generating encryption keys.

b) If encryption keys expire there shall be a documented process for managing the expiry of encryption keys.

c) There shall be a documented process to revoke encryption keys.

d) There shall be a documented process for securely changing the current encryption keyset.

e) There shall be a documented process in place for the storage of any encryption keys.

f) There shall be a method to recover data encrypted with a revoked or expired encryption key for a defined period of time after the encryption key becomes invalid.

11.19.5 SOFTWARE DEVELOPMENT LIFECYCLE.

The acquisition and development of new software shall follow defined processes in accordance with the information security policy.

a) The production environment shall be logically and physically separated from the development and test environments.

b) Development staff shall be precluded from having access to promote code changes into the production environment.

c) There shall be a documented method to verify that test software is not deployed to the production environment.

d) To prevent leakage of personally identifiable information, there shall be a documented method to ensure that raw production data is not used in testing.

e) All documentation relating to software and application development should be available and retained for the duration of its lifecycle.

11.19.6 CHANGE CONTROL.

The implementation of changes to the hardware and software of the Wireless Gaming System shall be managed by the use of formal change control procedures in accordance with the information security policy.

a) Program change control procedures shall be adequate to ensure that only properly approved and tested versions of programs are implemented on the production Wireless Gaming System. Production change controls shall include:

   i. An appropriate software version control or mechanism for all software components;

   ii. Details of the reason for the change;

   iii. Details of the person making the change;

   iv. Complete backups of previous versions of software;

   v. A policy addressing emergency change procedures;

   vi. Procedures for testing and migration of changes;

   vii. Segregation of duties between the developers, quality assurance team, the migration team and users; and

   viii. Procedures to ensure that technical and user documentation is updated as a result of a change.

b) All patches should be tested whenever possible on a wireless gaming system configured identically to the target wireless gaming system. Under circumstances where patch testing cannot be thoroughly conducted in time to meet the timelines for the severity level of the alert, then patch testing should be risk managed, either by isolating or removing the untested wireless gaming system from the network or applying the patch and testing after the fact.

11.19.7 INCIDENT MANAGEMENT.

A process for reporting information security incidents and the Management response shall be documented in accordance with the information security policy.

a) The incident management process shall include a definition of what constitutes an information

security incident.

b) The incident management process shall document how information security incidents are reported through appropriate management channels.

c) The incident management process shall address Management responsibilities and procedures to ensure a rapid, effective, and orderly response to information security incidents, including:

i. Procedures to handle different types of information security incident;

ii. Procedures for the analysis and identification of the cause of the incident;

iii. Communication with those affected by the incident;

iv. Reporting of the incident to the appropriate authority;

v. Forensic evidence collection; and

vi. Controlled recovery from information security incidents.

11.19.8 BUSINESS CONTINUITY AND DISASTER RECOVERY.

A plan shall be in place to recover gaming operations in the event that the production gaming system is rendered inoperable.

a) The disaster recovery plan shall address the method of storing player account information and gaming data to minimize loss in the event the production gaming system is rendered inoperable. If asynchronous replication is used, the method for recovering data should be described or the potential loss of data should be documented.

b) The disaster recovery plan shall delineate the circumstances under which it will be invoked.

c) The disaster recovery plan shall address the establishment of a recovery site physically separated from the production site.

d) The disaster recovery plan shall contain recovery guides detailing the technical steps required to re-establish gaming functionality at the recovery site.

e) The business continuity plan shall address the processes required to resume administrative operations of gaming activities after the activation of the recovered platform for a range of scenarios appropriate for the operational context of the Wireless Gaming System.

11.20 TECHNICAL CONTROLS

11.20.1 SELF MONITORING.

a) The Wireless Gaming System shall implement the self-monitoring of critical components (e.g., central hosts, network devices, firewalls, links to third parties, etc.).

b) A critical component which fails self-monitoring tests shall be taken out of service immediately. The component shall not be returned to service until there is reasonable evidence that the fault has been rectified.

c) The network should be redundant so that following b) above will not result in a denial of service condition

11.20.2 DOMAIN NAME SERVICE (DNS) REQUIREMENTS.

a) The primary server used to resolve DNS queries used in association with the Wireless Gaming System shall be physically located in a secure data center;

b) Logical and physical access to the primary DNS server shall be restricted to authorized personnel;

c) Zone transfers to arbitrary hosts shall be disallowed.

11.20.3 MONITORING.

a) The clocks of all components of the Wireless Gaming System shall be synchronized with an agreed accurate time source to ensure consistent logging. Time skew shall be checked periodically.

b) Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an appropriate period to assist in future investigations and access control monitoring.

c) System Administrator and System Operator activities shall be logged.

d) Logging facilities and log information shall be protected against tampering and unauthorized access.

e) Any modification, attempted modification, read access or other change or access to any Wireless Gaming System record, audit or log shall be detectable by the Wireless Gaming System. It shall be possible to see who has viewed or altered a log and when.

f) Logs generated by monitoring activities shall be reviewed periodically using a documented process. A record of each review shall be maintained.

g) Wireless Gaming System faults shall be logged, analyzed, and appropriate action taken.

h) Network appliances with limited onboard storage shall disable all communication if the audit log becomes full or offload logs to a dedicated log server.

11.20.4 CRYPTOGRAPHIC CONTROLS.

A policy on the use of cryptographic controls for protection of information should be developed and implemented.

a) Any sensitive or personally identifiable information should be encrypted if it traverses a network with a lower level of trust.

b) Data that is not required to be hidden but shall be authenticated shall use some form of message authentication technique.

c) Authentication shall use a security certificate from an approved organization.

d) The grade of encryption used should be appropriate to the sensitivity of the data.

e) The use of encryption algorithms shall be reviewed periodically by qualified Management staff to verify that the current encryption algorithms are secure.

f) Changes to encryption algorithms to correct weaknesses shall be implemented as soon as practical. If no such changes are available, the algorithm shall be replaced.

g) Encryption keys shall not be stored without being encrypted themselves through a different encryption method and/or by using a different encryption key.

11.20.5 ACCESS CONTROLS.

The allocation of access privileges shall be restricted and controlled based on business requirements and the principle of least privilege.

a) A formal user registration and de-registration procedure shall be in place for granting and revoking access to all information systems and services.

b) All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.

c) The use of generic accounts shall be limited, and where used the reasons for their use shall be formally documented.

d) Password provision shall be controlled through a formal management process.

e) Passwords shall meet business requirements for length, complexity and lifespan.

f) Access to Wireless Gaming System applications and operating systems shall be controlled by a secure log-on procedure.

g) Appropriate authentication methods, in addition to passwords, shall be used to control access by remote users.

h) Any physical access to areas housing Wireless Gaming System components, and any logical access to the Wireless Gaming System applications or operating system shall be recorded.

i) The use of automated equipment identification to authenticate connections from specific locations and equipment shall be formally documented and shall be included in the regular review of access rights by Management.

j) Restrictions on connection times shall be used to provide additional security for high-risk applications.

k) The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

l) A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.

m) Telecommuting into the Wireless Gaming System shall not be permitted except under circumstances where the security of the endpoint can be guaranteed.

11.20.6 NETWORK SECURITY MANAGEMENT.

Networks should be logically separated such that there should be no network traffic on a network link which cannot be serviced by hosts on that link.

a) The failure of any single item should not result in a denial of service.

b) An Intrusion Detection System / Intrusion Prevention System shall be installed on the network which can:

   i. Listen to both internal and external communications

   ii. Detect or prevent Distributed Denial of Service (DDOS) attacks

   iii. Detect or prevent shellcode from traversing the network

   iv. Detect or prevent Address Resolution Protocol (ARP) spoofing

v. Detect other Man-in-the-Middle indicators and sever communications immediately if detected

vi. Scan the wireless network for any unauthorized or rogue wireless devices connected to any access point on the wireless network. This scan should be performed at least once per quarter or as required by the CNGC.

vii. Scan the wireless network for any rogue access points. This scan should be performed at least once per quarter or as required by the CNGC.

viii. Automatically disable any unauthorized or rogue wireless devices connected to the system.

ix. Maintain a history log of all wireless access for at least the previous 90 days or a period as defined by the CNGC. This log should contain complete and comprehensive information about all wireless devices involved, and should be able to be reconciled with all other networking devices within the Gaming Venue or property.

c) In virtualized environments, redundant server instances cannot run under the same hypervisor.

d) Stateless protocols (e.g., UDP) should not be used for sensitive data without stateful transport.

NOTE: Although HTTP is technically stateless, if it runs on TCP which is stateful, this is allowed.

e) All changes to network infrastructure (e.g., network device configuration) shall be logged.

f) Virus scanners and/or detection programs should be installed on all pertinent information systems. These programs should be updated regularly to scan for new strains of viruses.

g) Network security should be tested by a qualified and experienced individual on a regular basis.

h) Testing should include testing of the external (public) interfaces and the internal network.

i) Testing of each security domain on the internal network should be undertaken separately.

11.20.7 FIREWALLS.

a) A firewall should be located at the boundary of any two dissimilar security domains.

b) All connections to Wireless Gaming System hosts in the secure data center shall pass through at least one application-level firewall. This includes connections to and from any non- Wireless Gaming System hosts used by the operator.

c) The firewall shall be a separate hardware device with the following characteristics:

i. Only firewall-related applications may reside on the firewall; and

ii. Only a limited number of accounts may be present on the firewall (e.g. system administrators only).

d) The firewall shall reject all connections except those that have been specifically approved.

e) The firewall shall reject all connections from destinations which cannot reside on the network from which the message originated (e.g., RFC1918 addresses on the public side of an internet firewall.)

f) The firewall shall maintain an audit log of all changes to parameters which control the connections permitted through the firewall.

g) The firewall shall maintain an audit log of all successful and unsuccessful connection attempts. Logs should be kept for 90 days, and a sample reviewed monthly for unexpected traffic. It is recommended that the source and destination IP addresses be recorded for each instance.

h) The firewall shall disable all communication if the audit log becomes full.

i) The number of unsuccessful connection attempts threshold shall be a configurable parameter by the network operator; and may be utilized to deny further connection requests should the threshold be exceeded. Should this threshold be exceeded, the operator shall be notified.

11.20.8 REMOTE ACCESS.

Remote access is defined as any access from outside the system or system network including any access from other networks within the same establishment. Remote access shall only be allowed if authorized by the CNGC and shall have the option to be disabled. Where allowed, remote access shall accept only the remote connections permissible by the firewall application and Wireless Gaming System settings. Remote access security will be reviewed on a case-by-case basis, in conjunction with the implementation of the current technology and approval from the CNGC. In addition, there shall be:

a) No unauthorized remote user administration functionality (adding users, changing permissions, etc.);

b) No unauthorized access to any database other than information retrieval using existing functions;

c) No unauthorized access to the operating system; and

d) The Wireless Gaming System shall maintain an activity log which updates automatically depicting all remote access information as follows:

i. Name of associate authorizing access;

ii. Name of authorized associate or manufacturer representative;

iii. Reason for access;

iv. Description of work performed; and

v. Date, time, and duration of access.

11.20.9 BACKUP.

Backup copies of information and software shall be taken and tested regularly in accordance with the backup policy.

11.21 PHYSICAL AND ENVIRONMENTAL CONTROLS

11.21.1 SECURE AREAS.

Wireless Gaming Systems and the associated communications systems shall be located in facilities which provide physical protection against damage from fire, flood, hurricane, earthquake, and other forms of natural or man-made disaster.

a) Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas which contain Wireless Gaming System components.

b) Secure areas shall be protected by appropriate entry controls to ensure that access is restricted to only authorized personnel.

c) All access shall be recorded in a secure log.

d) Secure areas shall include an intrusion detection system, and attempts at unauthorized access shall be logged.

11.21.2 GAMING EQUIPMENT SECURITY.

Wireless Gaming System servers shall be located in a secure area which restricts unauthorized access.

11.21.3 SUPPORTING UTILITIES.

a) All Wireless Gaming System components shall be provided with adequate primary power.

b) All Wireless Gaming System components responsible for the logical operations or data storage

of the system shall have Uninterruptible Power Supply (UPS) equipment to support operations in the event of a power failure.

c) There shall be adequate cooling and fire protection for the Wireless Gaming System components.

d) Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

Glossary

Reference	Definition
Active Directory	Active Directory is an implementation of LDAP directory services by Microsoft for use in Windows environments
AES	Advance Encryption standards
CCMP	Counter Mode CBC MAC Protocol
Client Software	The software installed on a Wireless Client Device that facilitates communication between the Player or Operator Interface to the Wireless Gaming System. Examples of Client Software include proprietary download software packages, html, flash, etc.
Default accounts	User accounts with predefined access levels usually created by default at installation for operating systems, databases, and applications.
Digital Certificate	A set of data which can be used to verify the identity of an entity by reference to a trusted third party (the Certification Authority). Digital certificates are often used to authenticate messages for non-repudiation purposes. One of the attributes of a digital certificate is that it cannot be modified without compromising its internal consistency. X.509 certificates are an example of a digital certificate.
Domain Name Service	The globally distributed Internet database which (amongst other things) maps machine names to IP numbers and vice-versa.
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol- Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol- Tunneled Transport Layer Security
Effective Bandwidth	The amount of data that actually can be transferred across a network per unit of time. The effective bandwidth through the Internet is usually considerably lower than the bandwidth of any of the constituent links
FIPS	Federal information Processing Standard
Firewall	Network security barrier. A firewall is a device that guards the entrance to a private network and keeps out unauthorized or unwanted traffic.
Generic user accounts	User accounts that are shared by multiple users (using the same password) to gain access to any component of a gaming system: application, database, or operating system.
GMK	Group Master Key
HTTP	Hypertext Transport Protocol
IEEE	Institute of Electrical and Electronics Engineers
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
Link Utilization	The percentage time that a communications link is engaged in transmitting data.

MAC	Medium Access Control
PEAP	Protected Extensible Authentication Protocol
PMK	Pairwise Master Key
Protocol	Used to refer to the hardware interface, line discipline and message formats of the communications
PTK	Pairwise Transient Key
RADIUS	Remote Authentication Dial In User Service
Sensitive Data	Data which, if obtained by a third party, may be used to affect game outcome/s or player/s accounts.
Service accounts	Accounts on which automated system functions are dependent to execute. These accounts defined at the operating system level provide a certain level of access necessary for normal operation of applications and/or automated batch processes.
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier, Network name
TKIP	Temporal key Integrity Protocol
Version Control	The method by which an evolving approved Wireless Gaming System is verified to be operating in an approved state.
VPN	Virtual Private Network
WAP	Wireless Access Point
WCD	Wireless Connectivity Devices
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity (WLAN)
Wireless Client Device	The device that converts communications from the Wireless Gaming System into a human interpretable form, and converts human decisions into communication format understood by the Wireless Gaming System. Examples of Wireless Client Devices include PDAs, mobile phones, tablets, etc. In some cases the Wireless Client Device may be a patron-owned device, while in other instances, it can be an operator-supplied device.
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

Revision History

February 17, 2023 – Updated CNGC Technical Standard to V4.5 using pre-industry release draft of GLI-26 V2.0 'Wireless System Standards', dated February 24, 2015, as well as content from the prior V4.4 of CNGC Technical Standards Chapter 11 – 'Wireless Networks'.

Amendments

CHOCTAW NATION OF OKLAHOMA

CHOCTAW NATION GAMING COMMISSION

AMENDMENT # 4

DATE MARCH 15, 2018

AMENDMENT TO TECHNICAL STANDARDS AND PROCEDURES FOR ELECTRONIC GAMING UNDER THE TRIBAL-OKLAHOMA STATE COMPACT AND 25 C.F.R. PART 547

This is an amendment to the Technical Standards issued by the Choctaw Nation Gaming Commission on January 8, 2018. The Section/s affected by this amendment is/are: 8.1.4 .

Amendment should be read as: 1) black font, normal script is the original language which remains unaffected by this amendment; 2) ~~red font, strikethrough script~~ is the original language removed pursuant to this amendment; 3) blue font, normal script is the new language inserted pursuant to this amendment.

SECTION/S AMENDED:

8.1.4 LINKED PLAYER INTERFACE ODDS.

Each device on the link shall have the same probability of winning the progressive, adjusted for the ~~denomination played~~ value of the wager. For the purpose of this requirement, "same" is defined as odds not exceeding a 5% difference and the payout percentage not exceeding a 1% difference. For instance, the probability shall remain the same for multiple denomination games based, on the monetary value of the wager (e.g., A two (2) coin $1 game has the probability of one (1) in 10,000 and a two (2) coin, $2 game on the same link has the probability one (1) in 5,000.)

SECTION AS AMENDED (FINAL):

8.1.4 LINKED PLAYER INTERFACE ODDS.

Each device on the link shall have the same probability of winning the progressive, adjusted for the value of the wager. For the purpose of this requirement, "same" is defined as odds not

exceeding a 5% difference and the payout percentage not exceeding a 1% difference. For instance, the probability shall remain the same for multiple denomination games based, on the monetary value of the wager (e.g., A two (2) coin $1 game has the probability of one (1) in 10,000 and a two (2) coin, $2 game on the same link has the probability one (1) in 5,000.)

CNGC Official:

	3-15-2018
Signature	Date
Michael Robison	
Print	

CHOCTAW NATION OF OKLAHOMA

CHOCTAW NATION GAMING COMMISSION

AMENDMENT # 3

DATE JANUARY 8, 2018

AMENDMENT TO TECHNICAL STANDARDS AND PROCEDURES FOR ELECTRONIC GAMING UNDER THE TRIBAL-OKLAHOMA STATE COMPACT AND 25 C.F.R. PART 547

This is an amendment to the Technical Standards issued by the Choctaw Nation Gaming Commission on August 20, 2013. The Section/s affected by this amendment is/are: 5.2.49.

Amendment should be read as: 1) black font, normal script is the original language which remains unaffected by this amendment; 2) ~~red font, strikethrough script~~ is the original language removed pursuant to this amendment; 3) blue font, normal script is the new language inserted pursuant to this amendment.

SECTION/S AMENDED:

5.2.49 BONUS GAMES.

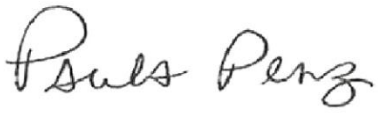
~~b) Each game which offers free games during game play (i.e., "fever" mode - a mode which gives the patron an opportunity for the following "X" number of hands to achieve a certain winning combination, with the pay-off being some number of bonus credits) should include the number of hands remaining for the free game event(s) as each free game is played;~~

SECTION AS AMENDED (FINAL):

5.2.49 BONUS GAMES.

b) Extended feature information: Each electronic game, which offers an extended feature (e.g., free games, re-spins, etc.), must display the number of feature games that remain during each game; except for extended features that are predetermined by the system (e.g. Class II server based systems).

CNGC Official:



	01-08-2018
Signature	Date

Paula Penz

Print

CHOCTAW NATION OF OKLAHOMA

CHOCTAW NATION GAMING COMMISSION

AMENDMENT # 2

DATE AUGUST 20, 2013

AMENDMENT TO TECHNICAL STANDARDS AND PROCEDURES FOR ELECTRONIC GAMING UNDER THE TRIBAL-OKLAHOMA STATE COMPACT AND 25 C.F.R. PART 547

This is an amendment to the Technical Standards issued by the Choctaw Nation Gaming Commission on May 23, 2012. The Section/s affected by this amendment is/are: 5.2.18 .

Amendment should be read as: 1) black font, normal script is the original language which remains unaffected by this amendment; 2) ~~red font, strikethrough script~~ is the original language removed pursuant to this amendment; 3) blue font, normal script is the new language inserted pursuant to this amendment.

SECTION/S AMENDED:

5.2.18 WRITABLE PROGRAM STORAGE.

iv) Does not allow game play while the media containing the critical data, files, and programs is in a modifiable state, unless otherwise approved by the Choctaw Nation Gaming Commission; and

SECTION AS AMENDED (FINAL):

5.2.18 WRITABLE PROGRAM STORAGE.

iv) Does not allow game play while the media containing the critical data, files, and programs is in a modifiable state, unless otherwise approved by the Choctaw Nation Gaming Commission; and

CNGC Official:

Kyle Norman

Signature

August 20, 2013

Date

Kyle Norman

Print

CHOCTAW NATION OF OKLAHOMA

CHOCTAW NATION GAMING COMMISSION

AMENDMENT # 1

DATE MAY 23, 2012

AMENDMENT TO TECHNICAL STANDARDS AND PROCEDURES FOR ELECTRONIC GAMING UNDER THE TRIBAL-OKLAHOMA STATE COMPACT AND 25 C.F.R. PART 547

This is an amendment to the Technical Standards issued by the Choctaw Nation Gaming Commission on May 7, 2012. The Section/s affected by this amendment is/are: 7.47.7 .

Amendment should be read as: 1) black font, normal script is the original language which remains unaffected by this amendment; 2) ~~red font, strikethrough script~~ is the original language removed pursuant to this amendment; 3) blue font, normal script is the new language inserted pursuant to this amendment.

SECTION/S AMENDED:

7.47.7 REQUIRED ELECTRONIC METERS.

The terminal/client and TCSS Server shall meet the requirements of Section ~~5.2.56 *Required Electronic Meters*~~ 5.2.37 *Electronic Accounting and Occurrence Meters*.

SECTION AS AMENDED (FINAL):

7.47.7 REQUIRED ELECTRONIC METERS.

The terminal/client and TCSS Server shall meet the requirements of Section 5.2.37 *Electronic Accounting and Occurrence Meters.*

CNGC Official:

Kyle Norman

Signature

5-23-12

Date

Kyle Norman

Print