STANDARD SERIES

GLI-14:

Finite Scratch Ticket and Pull-Tab Systems

Version: 2.2

Release Date: September 6, 2011

This Page Intentionally Left Blank

ABOUT THIS STANDARD

This Standard has been produced by **Gaming Laboratories International, LLC (GLI)** for the purpose of providing independent certifications to suppliers under this Standard and complies with the requirements set forth herein.

A supplier should submit equipment with a request that it be certified in accordance with this Standard. Upon certification, Gaming Laboratories International, LLC will provide a certificate of compliance evidencing the certification to this Standard.

Table of Contents

CHAPTER 1

1.0 Overview - Standards for Finite Systems

1.1 Introduction

1.1.1 Finite Systems Defined. Finite systems allow patrons to play at a terminal where Electronic Scratch Tickets, Electronic Pull-Tabs or Game Outcomes, hereinafter 'Electronic Tickets', are purchased. The Central System randomly selects the Electronic Ticket from a Game Set and communicates the Electronic Ticket to the Player Terminal. The Player Terminal provides for a display of the predetermined game outcome, using numbers or symbols. The player is then paid according to the paytable on the Player Terminal.

1.1.2 Phases of Certification. The approval of a Finite System shall be certified in two phases:

a) Initial laboratory testing, where the laboratory will test the integrity of the system in conjunction with Player Terminals, in the laboratory setting with the equipment assembled; and
b) On-site certification where the communications and set up are tested on the property prior to implementation.

1.2 Acknowledgment of Other Standards Reviewed

1.2.1 General Statement. These Standards have been developed by reviewing and using portions of the documents from the organizations listed below. We acknowledge the regulators who have assembled these documents and thank them:

a) State Of Washington - Class III Gaming Compact;
b) Mohawk Tribe of New York; and

c) New York Lottery.

1.3 Purpose of Standard

1.3.1 ***General Statement.*** The purpose of this technical standard is as follows:

a) To eliminate subjective criteria in analyzing and certifying Finite System operation.

b) To only test those criteria which impact the credibility and integrity of gaming from both the revenue collection and game play point of view.

c) To create a standard that will insure that Finite Systems are fair, secure, and able to be audited and operated correctly.

d) To distinguish between local public policy and laboratory criteria. At GLI, we believe that it is up to each local regulatory body to set their public policy with respect to gaming.

e) To recognize that non-gaming testing (such as Electrical Testing) should not be incorporated into this standard but left to appropriate test laboratories that specialize in that type of testing. Except where specifically identified in the standard, testing is not directed at health or safety matters. These matters are the responsibility of the manufacturer, purchaser, and operator of the equipment.

f) To construct a standard that can be easily changed or modified to allow for new technology.

g) To construct a standard that does not specify any particular technology, method or algorithm. The intent is to allow a wide range of methods to be used to conform to the standards, while at the same time, to encourage new methods to be developed.

1.3.2 ***No Limitation of Technology.*** One should be cautioned that this standard should not be read in such a way that limits the use of future technology. The document should not be interpreted that if the technology is not mentioned, then it is not allowed. Quite to the contrary, as new technology is developed, we will review this standard, make changes, and incorporate new minimum standards for the new technology.

1.3.3 Scope of Standard. This standard will only govern Finite System requirements necessary to achieve certification when interfaced to Player Terminals, for the purpose of communicating mandatory security events and game information.

1.4 Other Documents That May Apply

1.4.1 General Statement. This standard covers the minimal requirements for Finite Systems and all associated components. The following additional standards may also apply:

a) Gaming Devices in Casinos (GLI-11)
b) Progressive Gaming Devices in Casinos (GLI-12);
c) On-Line Monitoring and Control Systems (MCS) and Validation Systems in Casinos (GLI-13);
d) Cashless Systems (GLI-16);
e) Bonusing Systems (GLI-17);
f) Promotional Systems (GLI-18);
g) Client-Server Systems (GLI-21); and
h) Individual Regulatory Body Minimum Internal Control Procedures.

1.5 Definitions

1.5.1 General Statement. The following are definitions for the terms used throughout this document:

a) "Central System" A Central System is a computer system that consists of a finite number of Electronic Tickets, a certain number of which, if randomly selected, entitle a player to prize awards at various levels. The Central System conducts random drawings of Electronic Tickets from a Game Set upon request from the Player Terminal, and then issues the selection to the Player Terminal for display and payment. Once the Player Terminal receives the Electronic Ticket that Electronic Ticket is "removed" from the Game Set and may not be re-used. The Central System may reside within one Player Terminal or reside separately and be utilized by multiple Player Terminals that use the same Game Set. Finite pools of tickets are added to the

Central System by CD, DVD, Flash memory devices, or may be downloaded from a remote system.

b) "Electronic Ticket" An Electronic Ticket is an electronic scratch ticket, electronic pull-tab or an electronic game outcome. An Electronic Ticket is a predetermined winning or losing outcome in electronic form, distributed on-demand from a finite number of game outcomes by a Central System. Each Ticket represents a chance from among the finite set of chances. Referred to throughout this document as 'Electronic Tickets'.

c) "Game Set" A Game Set is the entire pool of finite Electronic Tickets that contain pre-defined game results assigned under a unique serial number.

d) "Game Subset" A Game Subset is a further division of a Game Set into equal sizes following randomization, with each Game Subset also identified by a unique serial number.

e) "Game Outcome" Game Outcome refers to the notion that the Central System may relay to the Player Terminal the fact that the player has won or lost an amount based on the selection generated from a Game Set of winning amounts. The Player Terminal then displays the correct graphics to relay this information to the player. In the alternative, the Central System could download the graphics to relay this information to the player, although this imposes a greater download time.

f) "Player Terminal" A Player Terminal is an electronic computer terminal housed in a cabinet and equipped with player input devices (i.e., ticket / bill acceptor, coin acceptor, card reader, touchscreen, and/or buttons), a video monitor or screen, or physical reels, and output devices including a printer and possibly a hopper. The terminal may be free-standing, tabletop, or handheld. This terminal is utilized by the player to place wagers, play the game(s), or offer and win prizes (when applicable). The Player Terminal may receive game play information from a server, or make its own determination, and then it displays this information to the player. Game play and other functions may be separated in parts, where some components may be generated within or outside the Player Terminal (e.g., Player Terminal that functions within a system).

g) "Thin Client" A thin client is a computer (client) in client-server architecture networks which depends primarily on the central server for processing activities. The word "thin" refers to the small boot image which such clients typically require - perhaps no more than required to connect to a network and start up a dedicated web browser or "Remote Desktop" connection.

CHAPTER 2

2.0 Player Terminal Requirements

2.1 Authorized Games

2.1.1 ***General Statement.*** Players receive, after the payment of a fee, an Electronic Ticket. A player wins if his or her Electronic Ticket contains an award. There may be multiple awards in each game. Player Terminals, as authorized by this standard, shall only allow players to purchase and play Electronic Tickets. Authorized games for Electronic Ticket devices shall conform to the following standards:

a) Payment to Begin Play. A player may purchase an opportunity to play an Electronic Ticket at a Player Terminal by:
   i) Insertion of cash or coins;
   ii) Insertion of a ticket/voucher (ticket in);
   iii) Swiping of a magnetic strip card; or
   iv) Purchase made at a point of sale terminal.

b) Available Games and Game Rules. The available games shall be displayed on the Player Terminal. The rules of the game shall be displayed on the terminal's video screen and/or payglass (i.e., rules of play and all winning combinations).

c) Payglass/Video Display. Payglasses or video displays shall be clearly identified and shall accurately state the rules of the game and the award that will be paid to the player when the player obtains a specific win. The payglasses or video displays shall clearly indicate whether awards are designated in credits, currency, or some other unit. The Player Terminal shall reflect any change in award value, which may occur in the course of play. This may be accomplished with a digital display in a conspicuous location of the Player Terminal, and the terminal must clearly indicate as such. All paytable information should be able to be accessed by a player, prior to them purchasing an Electronic Ticket.

Payglasses or video displays shall not be certified if the information is inaccurate or may cause confusion. The "reasonable player" standard shall be used for evaluation.

d) Multi-Games. Multiple game themes may be selectable on any given Player Terminal.

e) Display of Game Results. After the player purchases an Electronic Ticket, the award on that ticket is revealed to the player. The player may or may not have to interact with the terminal to reveal the win/loss results, i.e., it is up to the specific regulatory body to determine if the game results must initially be covered or hidden. The results of the Electronic Ticket shall be shown to the player using the video display, physical spinning reels, or other appropriate means.

f) Accountability Following Play. Following play on a Player Terminal, the result shall be clearly displayed on the video or touchscreen along with any prizes which may have been awarded. Prizes may be dispensed in the form of:

i) Ticket/voucher (ticket out);

ii) Credits added to the terminal's credit meter;

iii) Coins / Tokens paid out via a hopper; or

iv) Cashless Account Transfer Out.

2.1.2 Cashless Systems Defined. Cashless systems allow players to play terminals defined in this standard through the use of a magnetic strip player card, which accesses a player's account at the host system in the casino. Funds may be added to this player cashless account via a cashier station or any supporting terminal (through the insertion of coins, ticket/vouchers, bills, and coupons). The account value can be reduced either through debit transactions, in smaller amounts at a Player Terminal or by cashing out at a cashier's cage. A Cashless system is characterized as a host system whereby a player maintains an electronic account on the Casino's host database. Usually a casino issues a patron a unique magnetic card and Personal Identification Number (PIN) in conjunction with a cashless account on the system's database, although any method of uniquely identifying patrons could be implemented. All monetary transactions between a supporting Player Terminal and the host must be secured either by card insertion into a magnetic card reader attached to the host and PIN entry or by other protected means. After the player's identity is confirmed, the terminal may present transfer options to the patron on the video display of the card reader, which requires selection using a

keypad/touchscreen before occurring. Such options would include how many credits they wish to "withdraw" and placed on the terminal they are playing. Some systems may move either a predefined amount or the player's entire balance to the terminal for play. Once play is complete the player may have the option to move some of the credits back to the player's account or cash out some credits. Other systems may require that the entire credit value be transferred back to the system.

It should be noted here, at the outset, that some readers may have heard the term "EFT," which stands for "Electronic Funds Transfer". While this term has been used in the gaming industry as a description for Cashless gaming, it is important to note that this document does not contemplate nor request opinions on transferring money from a credit card account or bank account (ATM) for use in gaming. The "account" as described here is an account set up at the local casino for the purpose of play at that casino. Players, casinos, and the system described here cannot access the banking system for any transaction contemplated.

NOTE: *"Smart Card" technology implementation will be evaluated on a case-by-case basis.*

2.1.3 ***Credit Redemption.*** An available credit balance may be collected from the Player Terminal by the player pressing the 'CASHOUT' button 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 CASHOUT button is pressed; or
f) An error condition, provided the error condition prevents a valid cashout which is not supported through some other means.

Special Note: Regulatory bodies should consider several key criteria for authorized games including overall payback percentages for a completed Game Set (i.e., Min and Max RTP),

Game Set and Game Subset size, Max Bet, Max Award, allowed denominations, etc. These criteria are outside the scope of this Standard but must be clearly defined by respective jurisdictional regulations.

2.2 Hardware Requirements

2.2.1 General Statement. Player Terminals, used in connection with a Central System, shall conform to the Machine Requirements established within GLI-11 'Gaming Devices in Casinos', applicable requirements contained in GLI-21 ('Client Server System Client Terminals'), as well as the rules throughout this section. Player Terminals shall not have hardware that determines the outcome of any Electronic Ticket or affect the order of Electronic Tickets as dispensed from the Central System.

2.2.2 Secure Connections: DES or Equivalent Data Encryption. Connections between all components of the Finite System shall only be through the use of secure communication protocols which are designed to prevent unauthorized access or tampering, employing Data Encryption Standards (DES) or equivalent encryption with secure seeds or algorithms.

2.2.3 Basic Player Terminal Requirements. Player Terminals used in connection with Electronic Ticket devices shall conform to the following minimum standards:

a) No Player Terminal shall be capable of being used as a stand-alone unit for the purposes of engaging in any game not permitted by this standard;
b) In addition to a video monitor or touchscreen, each Player Terminal may have one or more of the following: a bill acceptor, coin acceptor, hopper, printer, magnetic card reader, and buttons for activating the game and providing player input, including a means for the player making selections and choices in games;
c) Each Player Terminal shall have a nonvolatile backup memory or its equivalent, which shall be maintained in a secure compartment on each Player Terminal for the purpose of storing and preserving a redundant set of critical data which has been error-checked in

accordance with applicable rules of the regulatory body, and which data shall include, at a minimum, the following Player Terminal information:

i) Electronic meters specified in the 'Metering within the Player Terminal' section of this document;

ii) Recall of all wagers and other information (e.g., Electronic Ticket number, serial number of Game Set, etc.) associated with the last ten (10) plays; and

iii) Error conditions that may have occurred on the Player Terminal which include:

A) NV memory error (for any critical memory) or Control Program error;

B) Low NV memory battery, for batteries external to the NV memory itself, or low power source;

C) Program error or authentication mismatch; and

D) Power reset.

d) An on/off switch that controls the electrical current that supplies power to the Player Terminal, which must be located in a secure place that is readily accessible within the interior of the Player Terminal;

e) All hardware switches and jumpers shall be fully documented for evaluation by the test laboratory. Hardware switches and/or jumpers which may alter the jurisdictional-specific configuration settings, paytables, game denomination, or payout percentages must meet configuration settings specified elsewhere in this standard and must be housed within a logic compartment of the Player Terminal. This includes top award changes (including progressives), selectable settings, or any other option that would affect payout percentage.

NOTE: It is permissible for critical memory and/or backup data storage to be contained on a server, provided it meets critical memory requirements contained in GLI-21.

2.2.4 Player Terminal Security. The Player Terminal shall be robust enough to withstand forced entry which would leave behind physical evidence of the attempted entry, or such entry causes an error code that is displayed and transmitted to the Central System, and which inhibits

game play until cleared, and which does not affect the subsequent play or any other play, prize or aspect of the game.

2.2.5 Player Terminal Wiring. The Player Terminal shall be designed so that power and data cables into and out of the Player Terminal 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 be securely fastened within the interior of the terminal.

Note: The Laboratory will make no determination as to whether the Player Terminal installation conforms to local electrical codes, standards and practices.

2.2.6 Player Terminal Identification. A Player Terminal shall have an identification badge affixed to the exterior of the cabinet by the manufacturer, that is not removable without leaving evidence of tampering, and this badge shall include the following information:

a) The manufacturer;
b) A unique serial number;
c) The Player Terminal model number; and
d) The date of manufacture;

2.2.7 Power Surges. The Player Terminal shall not be adversely affected, other than resets, by surges or dips of ± 20% of the supply voltage.

Note: It is acceptable for the equipment to reset provided no damage to the equipment or loss or corruption of data is experienced in the field. Upon reset, the Player Terminal must return to its previous state. It is acceptable for the terminal to return to a game completion state provided the game history and all credit and accounting meters constitute a completed game.

2.3 Diverter and Drop Box Requirements

2.3.1 ***Diverter***. For Player Terminals that accept coins or tokens, the software shall ensure that the diverter directs coins to the hopper, or to the drop box when the hopper is full. The hopper full detector shall be monitored to determine whether a change in diverter status is required. If the state of the detector changes, the diverter shall operate as soon as possible, or within ten (10) games, after the state change, without causing a disruption of coin flow, or creating a coin jam. Hopper-less terminals shall always divert coins to the drop box.

2.3.2 ***Drop Box***. If the Player Terminal is equipped to accept coins or tokens, then the following rules shall be met:

a) Each terminal equipped to accept coins or tokens shall contain a separate drop bucket or drop box to collect and retain all such coins or tokens that are diverted into the drop box;
b) A drop bucket shall be housed in a locked compartment separate from any other compartment of the Player Terminal; and
c) There must be a method to monitor the drop box area, even if manufactured by a different company. It is preferred that the monitoring method provide for notification to the Central System.

2.4 External Doors/Compartments and the Logic Door / Logic Area

2.4.1 ***External Doors/Compartments***. Each Player Terminal shall have a locked external front door in which the interior of the terminal shall not be readily accessible when such door is in the closed, locked position. The following rules shall apply to the Player Terminal's external doors:

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

b) All external doors shall be locked and monitored by door access sensors, which shall detect and report all external door openings to the Player Terminal by way of an audible alarm, on-screen display, or both;

c) The Player Terminal shall cease play when any external door is opened;

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

e) The sensor system shall register a door as being open when the door is moved from its fully closed and locked position, provided power is supplied to the terminal; and

f) Door open conditions shall be recorded in an electronic log that includes a date/time stamp.

2.4.2 Logic Compartment. Player Terminals shall have a separate internal locked logic compartment which shall be keyed differently than the front door access lock. The logic compartment shall be a locked cabinet area (with its own locked door), which houses critical electronic components that have the potential to significantly influence the operation of the Player Terminal. There may be more than one (1) such logic area in a Player Terminal. The logic door shall be monitored. Electronic components that are required to be housed in one (1) or more logic areas are:

a) CPUs and any program storage device that contains software that may affect the integrity of gaming, including but not limited to the game accounting, system communication, and peripheral firmware devices involved in, or which significantly influence, the operation and calculation of game play, game display, game result determination, or game accounting, revenue, or security. Any exception will be evaluated on a case-by-case basis;

b) Communication controller electronics and components housing the communication program storage device. Any exceptions will be evaluated on a case-by-case basis;

c) The NV memory back-up device, if applicable, shall be kept within a locked logic area; and

d) Logic compartment door open conditions shall be recorded in a log that includes a date/time stamp.

2.5 Coin/Token and Currency Compartments

2.5.1 General Statement. The coin or token and currency compartments shall be locked separately from the main cabinet area. A separate coin/token compartment shall not be required for coins or tokens necessary to pay prizes in a Player Terminal that pays prizes through a hopper.

2.5.2 Access to Currency.

a) Access to the currency storage area is to be secured via separate key locks and shall be fitted with sensors that indicate door open/close and stacker receptacle removed, provided power is supplied to the terminal.

b) Access to the currency storage area is to be through two (2) levels of locks (the relevant outer door plus one other door or lock) before the currency can be removed.

2.6 Methods of Inserting Monetary Values into the Player Terminal

2.6.1 Coin / Token Acceptors. If the Player Terminal uses a coin / token acceptor, the acceptor shall accept or reject the coin / token on the basis of metal composition, mass, composite makeup, or an equivalent method to securely identify a valid coin/token. In addition, it shall meet the following rules:

a) Credit Meter Update on Coin / Token Insertion. Each valid coin / token inserted shall register the actual monetary value or the appropriate number of credits received for the denomination being used on the player's credit meter for the current game or bet meter. If registered directly as credits, the conversion rate shall be clearly stated, or be easily ascertainable from the Player Terminal.

b) Coin / Token Acceptor Security Features/Error Conditions. The coin acceptor shall be designed to prevent the use of cheating methods including, but not limited to, slugging (counterfeit coins), stringing (coin pullback), the insertion of foreign objects and any other manipulation that may be deemed as a cheating technique. Appropriate correlating error conditions should be generated and the coin acceptor should be disabled;

c) Rapidly Fed Coins / Tokens. The Player Terminal shall be capable of handling rapidly-fed coins / tokens or piggy-backed coins / tokens so that occurrences of cheating are eliminated. Coins / Tokens traveling too fast that do not register on the player's credit meter should be returned to the player;

d) Direction Detectors. The Player Terminal shall have suitable detectors for determining the direction and the speed of coin / token travel in the receiver. If a coin / token traveling at too slow of a speed or improper direction is detected, the Player Terminal shall display a suitable error condition for at least thirty (30) seconds or be cleared by an attendant;

e) Invalid Coins / Tokens. Coins / tokens deemed invalid by the acceptor shall be rejected to the coin tray and shall not be counted as credits;

f) Coin / Token Acceptor Error Conditions. Coin / Token acceptors shall have a mechanism to allow software to interpret and act upon the following conditions:

   i) Token or coin-In jam
   ii) Coin return jam
   iii) Reverse token or coin-in (coin / token traveling wrong direction through acceptor); and
   iv) Token or coin too slow

Note: It is acceptable to report coin-in jam, reverse coin-in and coin too slow as a generic coin-in error.

2.6.2 ***Bill Validators.*** All paper currency acceptance devices shall be able to detect the entry of valid bills, coupons, ticket/vouchers, or other approved notes, as applicable, and provide a method to enable the Player Terminal software to interpret and act appropriately upon a valid or invalid input. The paper currency acceptance device(s) shall be electronically-based and be

configured to ensure that they only accept valid bills of legal tender, coupons, ticket/vouchers, or other approved notes, and must reject all other items. Rejected bills, ticket/vouchers, coupons or other approved notes should be returned to the player. Ticket/vouchers are paper slips that are treated as a unit of currency, which may be redeemed for cash or exchanged for credits on the Player Terminal. Coupons are paper slips primarily used for promotional purposes, which may be of a cashable or non-cashable value. 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 meet the following rules for all acceptable types of medium:

a) Each valid bill, coupon, ticket/voucher or other approved note shall register the actual monetary value or the appropriate number of credits received for the denomination being used on the player's credit meter.

b) Credit meter update upon bill insertion. Credits shall only be registered when:
   i) The bill or other note has passed the point where it is accepted and stacked; and
   ii) The acceptor has sent the "irrevocably stacked" message to the Player Terminal.

c) Bill validator security features. Each bill validator shall be designed to prevent the use of cheating methods such as stringing, the insertion of foreign objects and any other manipulation that may be deemed as a cheating technique. A method for detection of counterfeit bills must be implemented;

d) Credit acceptance conditions. Acceptance of any bills, ticket/vouchers, coupons or other approved notes for crediting to the credit meter shall only be possible when the Player Terminal is enabled for play. Other states, such as error conditions, including door opens, audit mode and game play, shall cause the disabling of the bill validator system; with the exception of allowing credit acceptance during game play for terminals that allow players to place bets on upcoming events (e.g. horse racing wagering);

e) Bill validator error conditions. Each Player Terminal and/or bill validator shall have the capability of detecting and displaying the following error conditions, and shall cause the Player Terminal and/or the bill validator to lock up and require attendant intervention to clear:

i. Stacker full - It is recommended that an explicit "stacker full" error message not be utilized since this may promote a security issue. Rather, a message such as "Bill Validator Malfunction" or similar is suggested.);
ii. Bill jams;
iii. Stacker door open (this is the door immediately prior to accessing the cashbox/stacker assembly);
iv. Stacker removed; and
v. Bill validator malfunction not specified above.

2.6.3 ***Communications.*** All bill validators shall communicate to the Player Terminal using a bi-directional protocol.

2.6.5 ***Factory Set Ticket / Bill Validators***. If bill validators are designed to be factory set only, it shall not be possible to access or conduct maintenance or adjustments to those bill validators in the field, other than:

a) The selection of bills, coupons, ticket/vouchers, or other approved notes and their limits;
b) Changing of certified control program media or downloading of certified software;
c) Adjustment of the bill validator for the tolerance level for accepting tickets and bills of varying quality should not be allowed externally to the Player Terminal. Adjustments of the tolerance level should only be allowed with adequate levels of security in place. This can be accomplished through lock and key, physical switch settings, or other accepted methods approved 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 ticket and/or bill acceptance.

2.6.6 ***Tokenization.*** For Player Terminals that allow tokenization, the terminal shall receive monetary value from the bill or coin acceptor and post to the player's credit meter the entire amount inserted and display any fractional credits when applicable. It is acceptable for the terminal to store the fractional credits if one of the following conditions is met:

a) The Player Terminal displays the credit meter in dollars and cents; or

b) The Player Terminal informs the player that there are fractional credits stored on the terminal at an opportune time to avoid the possibility of the player walking away from the terminal without such knowledge.

Note: See also GLI-16, Cashless Systems for Casinos, for detailed requirements related to cashless environments.

2.6.7 Accountability of Tickets and Bills Accepted. A Player Terminal, which contains a bill validator device, shall maintain sufficient electronic metering to be able to display 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;

d) For all other notes (ticket/vouchers and coupons), the Player Terminal shall have a separate meter that reports the number of items accepted, not including bills.

2.6.8 Bill Validator Recall. A Player Terminal that uses a bill validator shall retain in its memory and display the above-required information of the last five (5) items accepted by the bill validator (i.e., currency, ticket/vouchers, coupons, etc.) The bill validator recall log may be combined or maintained separately by item type. If combined, the type of item accepted shall be recorded with the respective timestamp.

2.6.9 Bill Validator Stacker Requirements. Each bill validator shall have a secure stacker and all accepted items shall be deposited into the secure stacker. The secure stacker and its receptacle are to be attached to the Player Terminal in such a manner so that they cannot be easily removed by physical force and shall meet the following rules:

a) The bill validator device shall have the ability to detect a stacker full condition; and

b) There shall be a separate keyed lock to access the stacker area. This keyed lock shall be separate from the main door. In addition, a separate keyed lock shall be required to remove the bills from the stacker.

2.6.10 Bill Validator Location. If a Player Terminal is equipped with a bill validator, it shall be located in a locked area of the terminal (e.g., require opening of the main door to access), but not in the logic area. Only the bill or ticket/voucher insertion area will be accessible by the player.

2.7 Coin / Token Hoppers

2.7.1 General Statement. If coin / token hoppers are used, they are to be monitored, in all game states, by the Player Terminal control program. Coin / token hoppers shall prohibit manipulation by the insertion of a light source or any foreign object and there shall not be an abnormal payout when exposed to higher levels of electro-static discharge or if power is lost at any time during a payout.

Note: Activities that result in the payout of a single extra coin (e.g. the removal and re-insertion of the hopper) are not considered an abnormal payout as long as it is accounted for as an extra coin paid.

2.7.2 Acceptable Hopper Locations. If a Player Terminal is equipped with a hopper it shall be located in a locked area of the terminal, but not in the logic area or the drop box. Access to the hopper shall require at a minimum opening of a secure external door.

2.7.3 Hopper Error Conditions. A Player Terminal that is equipped with a hopper shall have mechanisms to allow control program software to interpret and act upon the following conditions:

a) Hopper empty or timed out;
b) Hopper jam; and
c) Hopper runaway or extra coin paid out.

2.8 Printers

2.8.1 ***Payment By Printers***. If the Player Terminal has a printer that is used to make payments, the terminal may pay the player by issuing a printed ticket/voucher. The printer shall print on a ticket/voucher and the Player Terminal shall support the transmission of data to an on-line data system that records the following information regarding each payout ticket/voucher printed. The information listed below can be obtained from the Player Terminal, interface board, the on-line data management system, or another means:

a) Value of credits in local monetary units in numerical form;
b) Time of day the ticket/voucher was printed in twenty-four (24) hour format showing hours and minutes – printing of this information is not required, provided that storage of this information is in the database;
c) Date, in any recognized format, indicating the day, month, and year;
d) Player Terminal number or machine number;
e) Unique validation number (including a copy of the validation number on the leading edge of the ticket/voucher);
f) Barcode (not required for ticket/vouchers that are non-redeemable at a Player Terminal); and
g) If offline voucher issuance is supported, an offline authentication identifier must, at-a-minimum, be printed on the immediate next line following the leading edge validation number that in no way overwrites, or otherwise compromises, the printing of the validation number on the ticket (not required for ticket/vouchers that are non-redeemable at a Player Terminal). The offline authentication identifier must be derived by a hash, or other secure encryption method of at least 128 bits, that will uniquely identify the voucher, verify that the redeeming system was also the issuing system, and validate the amount of the voucher. For cases where a suitable authentication identifier is not printed on the voucher, the Player Terminal must print at most one wagering instrument after the terminal to system communications have been lost.

To further meet the above requirement, the Player Terminal shall either keep a duplicate copy or print only one (1) copy to the player but have the ability to retain the last twenty-five (25) ticket/voucher-out information* to resolve player disputes. In addition, an approved system shall be used to validate the payout ticket/voucher, and the ticket/voucher information on the Central System shall be retained at least as long as the ticket/voucher is valid at that location. If offline voucher issuance is supported, the Player Terminal must mask all but the last 4 digits of the validation number as displayed in the twenty-five (25) ticket/voucher-out log.
(*The ticket/voucher-out log may contain ticket/vouchers and receipts.)

2.8.2 ***Printer Location.*** If a Player Terminal is equipped with a printer, it shall be located in a locked area of the terminal (i.e., require opening of a locked external door), but not be housed within the logic area or the drop box.

2.8.3 ***Printer Error Conditions*** A printer shall have mechanisms to allow control program software to interpret and act upon the following conditions:

a) Out of paper/paper low - It is permissible for the Player Terminal to not lock up for these conditions; however, there should be a means for the attendant to be alerted;
b) Printer jam/failure; and
c) Printer disconnected - It is permissible for the Player Terminal to detect this error condition when it tries to print.

2.9 Card Readers

2.9.1 ***Card Readers***, if applicable, must meet applicable requirements stated in GLI-16, Cashless Devices in Casinos, as well as the following requirements in this standard.

2.9.2 ***Audit Trails for Cashless Transactions***. Cashless Player Terminals must have the ability to recall the last twenty-five (25) monetary transactions received from the host system and the last twenty-five (25) monetary transactions transmitted to the host system. However, if a Player Terminal has promotional or host-bonusing features, or both, enabled simultaneously with

cashless features, a single 100-event log would suffice. The following information must be displayed:

a) The type of transaction (upload/download);

b) The transaction value;

c) The time and date; and

d) The player's account number or a unique Transaction Number, either of which can be used to authenticate the source of the funds (i.e. source of where funds came from/went to).

2.9.3 Meter Requirements for Cashless Player Terminals and Systems. Cashless devices (which includes Player Terminals supporting cashless functionality) and cashless host systems must incorporate electronic accounting meters that conform to the following electronic metering requirements. See also applicable requirements found in "Electronic Metering Within the Player Terminal".

a) The operation of the mandatory electronic accounting meters, as mandated in GLI-11, must not be impacted directly for cashless type transactions;

b) Specific cashless electronic accounting meters shall exist which should increment to indicate:
   i) electronic credits received from the Central System---downloaded to terminal from host.
   ii) electronic credits transmitted to the Central System---uploaded from terminal to host.

c) Meters shall be labeled so they can be clearly understood in accordance with their function.

2.9.4 Transaction Confirmation. The Player Terminal or host card reader display must be capable of providing confirmation/denial of every cashless transaction initiated. This confirmation/denial must include:

a) The type of transaction (upload/download);

b) The transaction value;

c) The time and date (if printed confirmation);

d) The player's account number or a unique Transaction Number, either of which can be used to authenticate the source of the funds (i.e. source of where funds came from/went to) [if printed confirmation]; and

e) A descriptive message as to why the transaction did not complete as initiated. This applies only to the denied transactions.

2.9.5 ***Error Conditions***. The following sections outline the Error Conditions that apply to the:

a) Host System. The following conditions must be monitored, and a message must be displayed to the patron at the host card reader for the following:
   i) invalid PIN or Player ID (Can Prompt for Re-entry up to maximum allowed); and
   ii) account unknown.

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

2.9.6 ***Transfer of Transactions***. If a player initiates a cashless transaction and that transaction would exceed terminal-configured limits (i.e. the credit limit, etc) then this transaction may only be processed provided that the patron is clearly notified that he has received or deposited less than requested to avoid patron disputes.

2.10 Video Monitor/Touchscreens

2.10.1 ***Video Monitor/Touchscreens***, if applicable, must meet the following rules:

a) Touchscreens shall be accurate once calibrated and shall maintain that accuracy for at least the manufacturer's recommended maintenance period;
b) A touchscreen should be able to be re-calibrated without access to the Player Terminal cabinet other than opening the main door; and
c) There shall be no hidden or undocumented buttons/touch points anywhere on the touchscreen that affect game play and/or that impact the outcome of the game, except as provided for by the game rules.

2.11 Software Requirements

2.11.1 ***General Statement.*** Player Terminal software shall conform to the Software Requirements established in GLI-11 'Gaming Devices in Casinos' with the exception of 'Mechanical and Electro-Mechanical Random Number Generator (RNG) Requirements.' The Player Terminal shall not have software that determines the outcome of any Electronic Ticket game. The result is determined by the Central System as outlined within this document.

2.11.2 ***Function of NV Memory Reset***. Following the initiation of an NV memory reset procedure (utilizing a certified NV memory clear method), the game program shall execute a routine, which initializes all bits in critical NV memory to the default state. All memory locations intended to be cleared as per the NV memory clear process shall be fully reset in all cases. For Player Terminals that allow for partial NV memory clears, the methodology in doing so must be accurate.

2.11.3 ***Default Reel Position or Game Display.*** The default reel position or game display immediately after an NV memory reset shall not be the advertised top award on any selectable line. The default game display, upon entering game play mode, shall also not be the advertised top award. This applies to the base game only and not to any secondary bonus features. This

does not apply to games or paytables selected after the initial game play.

2.11.4 Configuration Settings. It shall not be possible to change a configuration setting that causes an obstruction to the electronic accounting meters without an NV memory clear. Notwithstanding, a change to the denomination must be performed by a secure means, which includes access to the locked logic area or other secure method provided that the method can be controlled by the regulator (e.g., password or PIN-based controls).

2.11.5 Critical Memory Defined. Critical memory is used to store all data that is considered vital to the continued operation of the Player Terminal. This includes, but is not limited to:

a) All electronic meters required in 'Metering within the Player Terminal', including last bill data and power up and door open metering;
b) Current credits;
c) Player Terminal/game configuration data;
d) Information pertaining to the last ten (10) games with the game outcome (including the current game, if incomplete). Player Terminals offering games with a variable number of free games, per base game, may satisfy this requirement by providing the capability to display the last 50 free games in addition to each base game; and
e) Software state (the last normal state, last status, or tilt status the Player Terminal software was in before interruption);
f) Any paytable configuration information residing in memory; and
g) It is recommended that, at a minimum, a log of the last 100 significant events be kept in critical memory.

General Statement Critical memory storage shall be maintained by a methodology that enables errors to be identified. This methodology may involve signatures, checksums, partial checksums, multiple copies, timestamps and/or effective use of validity codes.

Special Note: The above is not intended to preclude the use of alternate storage media types, such as hard disk drives, for the retention of critical data. Such alternate storage media is still

expected to maintain critical data integrity in a manner consistent with the requirements in this section, as applicable to the specific storage technology implemented.

2.11.6 Comprehensive Checks. Comprehensive checks of critical memory shall be made following game initiation but prior to display of game outcome to the player. It is recommended that critical memory is continuously monitored for corruption. The methodology shall detect failures with an extremely high level of accuracy.

General Statement. An unrecoverable corruption of critical memory shall result in an error. The memory error should not be cleared automatically and should result in a tilt condition, which facilitates the identification of the error and causes the Player Terminal to cease further function. The critical memory error should also cause any communication external to the Player Terminal to immediately cease. An unrecoverable critical memory error shall require a full NV memory clear performed by an authorized person.

2.11.7 NV Memory and Program Storage Device Space. Non-volatile memory space that is not critical to Player Terminal security (e.g., video or sound) is not required to be validated.

2.12 Program Storage Device Requirements

2.12.1 General Statement. The term *Program Storage Device* is defined to be the media or an electronic device that contains the critical control program components. Device types include but are not limited to EPROMs, compact flash cards, optical disks, hard drives, solid state drives, USB drives, etc. This partial list may change as storage technology evolves.

All program storage devices shall:

a) Be housed within a fully enclosed and locked logic compartment;

b) Be clearly marked with sufficient information to identify the software and revision level of the information stored in the device. In the case of media types on which multiple programs may reside it is acceptable to display this information via the attendant menu;

c) Validate themselves during each processor reset;

d) Validate themselves the first time they are used; and

e) CD-ROM, DVD, and other optical disk-based Program Storage shall:

   i. Not be a re-writeable disk; and

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

2.13 Control Program Requirements

2.13.1 Control Program Verification.

a) EPROM-based Program Storage:

   i. Player Terminals which have control programs residing in one or more EPROMs must employ a mechanism to verify control programs and data. The mechanism must use, at a minimum, a checksum; however, it is recommended that a Cyclic Redundancy Check (CRC) be used (at least 16-bit).

b) Non-EPROM Program Storage shall meet the following rules:

   i. The software shall provide a mechanism for the detection of unauthorized and corrupt software elements, upon any access, and subsequently prevent the execution or usage of those elements by the Player Terminal. The mechanism must employ a hashing algorithm which produces a message digest output of at least 128 bits.

   ii. In the event of a failed authentication, after the Player Terminal has been powered up, the terminal should immediately enter an error condition and display an appropriate error. This error shall require operator intervention to clear and shall not clear until the data authenticates properly, following the operator intervention, or the media is replaced or corrected, and the Player Terminal's memory is cleared.

Note: Control Program Verification Mechanisms may be evaluated on a case-by-case basis and approved by the regulator and the independent testing laboratory based on industry standard security practices.

c) Alterable Media shall meet the following and additional rules:

i. Employ a mechanism which tests unused or unallocated areas of the alterable media for unintended programs or data and tests the structure of the media for integrity. The mechanism must prevent further play of the Player Terminal if unexpected data or structural inconsistencies are found.

ii. Employ a mechanism for keeping a record any time a control program component is added, removed, or altered on any alterable media. The record shall contain a minimum of the last ten (10) modifications to the media and each record must contain that date and time of the action, identification of the component affected, the reason for the modification and any pertinent validation information.

Note: Alterable Program Storage does not include memory devices typically considered to be alterable which have been rendered "read-only" by either a hardware or software means.

2.13.2 Program Identification. Program storage devices which do not have the ability to be modified while installed in the Player Terminal during normal operation, shall be clearly marked with sufficient information to identify the software and revision level of the information stored in the devices.

2.13.3 Independent Control Program Verification. The Player Terminal shall have the ability to allow for an independent integrity check of the terminal's software from an outside source and is required for all control programs that may affect the integrity of the game. This must be accomplished by being authenticated by a third-party device, which may be embedded within the game software (see NOTE below), by having an interface port for a third-party device to authenticate the media, or by allowing for removal of the media such that it can be verified externally. This integrity check will provide a means for field verification of the software to

identify and validate the program. The test laboratory, prior to device approval, shall evaluate the integrity check method.

Note: If the authentication program is within the game software, the manufacturer must receive written approval from the test prior to submission.

2.14 Electronic Metering Within the Player Terminal

2.14.1 Credit Meter Units and Display. The credit meter shall be maintained in credits or cash value (i.e. applicable local currency) and shall at all times indicate all credits or cash available for the player to wager or cashout with the exception of when the player is viewing an informational screen such as a menu or help screen item. This should be displayed to the player unless a tilt condition or malfunction exists.

2.14.2 Tokenization. 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 value, the credits displayed for that game may be displayed and played as a truncated amount, (i.e., fractional part removed). However, the fractional credit amount shall be made available to the player when the truncated credit balance is zero. The fractional amount is also known as 'Residual Credit'.

2.14.3 Credit Meter – Incrementing. The value of every prize at the end of a game shall be added to the player's credit meter, except for handpays or merchandise. The value of all prize(s) awarded shall be added to the player's credit meter, except for handpays or merchandise.

2.14.4 Progressives. Progressive awards may be added to the credit meter if either:

a) The credit meter is maintained in the local currency amount format; or
b) The progressive meter is incremented to whole credit amounts; or
c) The progressive prize in local currency amount format is converted properly to credits upon transfer to the player's credit meter in a manner that does not mislead the player

(i.e., make unqualified statement "wins meter amount" and then rounds down on conversion or cause accounting imbalances).

See also, GLI-12 Progressive Gaming Devices in Casinos.

2.14.5 Collect Meter. There shall be a collect meter, which will show the number of credits or cash, collected by the player upon a cashout**.** This should be displayed to the player unless a tilt condition or malfunction exists. The number of credits or cash collected shall be subtracted from the player's credit meter and added to the collect meter. This meter may include handpays.

2.14.6 Software Meter Information Access. The software meter information shall only be accessible by an authorized person and must have the ability to be displayed on demand using a secure means.

2.14.7 Electronic Accounting and Occurrence Meters. Electronic accounting meters shall be at least ten (10) digits in length. These meters shall be maintained in credit units equal to the denomination, or in dollars and cents. If the meter is being used in dollars and cents format, eight (8) digits must be used for the dollar amount and two (2) digits used for the cents amount. Player Terminals configured for multi-denomination play shall display the units in dollars and cents. The meter must roll over to zero upon the next occurrence, any time the meter exceeds ten (10) digits and after 9,999,999,999 has been reached or any other value that is logical. Occurrence meters shall be at least eight (8) digits in length however, are not required to automatically roll over. Meters shall be labeled so they can be clearly understood in accordance with their function. All Player Terminals shall be equipped with a device, mechanism or method for retaining the value of all meter information specified in this standard which must be preserved in the event of power loss to the terminal. The required electronic meters are as follows (accounting meters are designated with an asterisk '*'):

a) Coin In*. The Player Terminal must have a meter that accumulates the total value of all wagers, whether the wagered amount results from the insertion of coins, tokens, currency, 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. For all games, provide the coin in information, on a per paytable basis, to calculate a weighted average theoretical payback percentage; and

iii. For paytables with a difference in theoretical payback percentage which exceeds 4 percent between wager categories, the Player Terminal shall 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.

Note: Wager categories, as defined above, do not apply to Keno or Skill Games.

b) Coin Out*. The Player Terminal must have a meter that accumulates the total value of all amounts directly paid by the terminal 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 will not record amounts awarded as the result of an external bonusing system or a progressive payout;

c) Coin Drop*. The Player Terminal must have a meter that accumulates the total value of coins or tokens diverted to the drop;

d) Attendant Paid Jackpots*. The Player Terminal must have a meter that accumulates the total value of credits paid by an attendant resulting from a single game cycle, the amount of which is not capable of being paid by the terminal 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 specifically identified amounts listed in the manufacturer's par sheet. Jackpots which are keyed to the credit meter shall NOT increment this meter;

e) Attendant Paid Cancelled Credits*. The Player Terminal must have a meter that accumulates the total value paid by an attendant resulting from a player initiated cash-out that exceeds the physical or configured capability of the terminal to make the proper payout amount;

f) Physical Coin In*. The Player Terminal must have a meter that accumulates the total value of coins or tokens inserted into the terminal;

g) Physical Coin Out*. The Player Terminal must have a meter that accumulates the value of all coins or tokens physically paid by the terminal;

h) Bill In*. The Player Terminal must have a meter that accumulates the total value of currency accepted. Additionally, the terminal must have a specific occurrence meter for each denomination of currency accepted that records the number of bills accepted of each denomination;

i) Ticket and/or Voucher In*. The Player Terminal must have a meter that accumulates the total value of all Player Terminal vouchers accepted by the terminal; (A.K.A. Ticket-in) ;

j) Ticket and/or Voucher Out*. The Player Terminal must have a meter that accumulates the total value of all Player Terminal vouchers and payout receipts issued by the terminal (A.K.A. Ticket-Out);

k) Electronic Funds Transfer In* (EFT In). The Player Terminal must have a meter "EFT In" that accumulates the total value of cashable credits electronically transferred from a financial institution to the Player Terminal through a cashless wagering system;

l) Cashless Account Transfer In* (A.K.A. WAT In-Wagering Account Transfer In). The Player Terminal must have a meter that accumulates the total value of cashable credits electronically transferred to the terminal from a wagering account by means of an external connection between the terminal and a cashless wagering system;

m) Cashless Account Transfer Out* (A.K.A. WAT Out-Wagering Account Transfer Out). The Player Terminal must have a meter that accumulates the total value of cashable credits electronically transferred from the terminal to a wagering account by means of an external connection between the terminal and a cashless wagering system;

n) Non-Cashable Electronic Promotion In*. The Player Terminal must have a meter that accumulates the total value of non-cashable credits electronically transferred to the terminal from a promotional account by means of an external connection between the terminal and a cashless wagering system;

o) Cashable Electronic Promotion In*. The Player Terminal must have a meter that accumulates the total value of cashable credits electronically transferred to the terminal

from a promotional account by means of an external connection between the terminal and a cashless wagering system;

p) Non-Cashable Electronic Promotion Out*. The Player Terminal must have a meter that accumulates the total value of non-cashable credits electronically transferred from the terminal to a promotional account by means of an external connection between the terminal and a cashless wagering system;

q) Cashable Electronic Promotion Out*. The Player Terminal must have a meter that accumulates the total value of cashable credits electronically transferred from the terminal to a promotional account by means of an external connection between the terminal and a cashless wagering system;

r) Cashable Promotional Credit Wagered. The Player Terminal must have a meter that accumulates the total value of promotional cashable credits which are wagered. This includes credits that are transferred to the terminal electronically or through the acceptance of coupon or voucher;

s) Coupon Promotion In*. The Player Terminal must have a meter that accumulates the total value of all promotional coupons accepted by the terminal;

t) Coupon Promotion Out*. The Player Terminal must have a meter that accumulates the total value of all promotional coupons issued by the terminal;

u) Machine Paid External Bonus Payout*. The Player Terminal must have a meter that accumulates the total value of additional amounts awarded as a result of an external bonusing system and paid by the terminal;

v) Attendant Paid External Bonus Payout*. The Player Terminal must have a meter that accumulates the total value of amounts awarded as a result of an external bonusing system paid by an attendant. Bonus payouts which are keyed to the credit meter, shall not increment this meter;

w) Attendant Paid Progressive Payout*. The Player Terminal must 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 terminal itself. Progressive payouts which are keyed to the credit meter shall not increment this meter;

x) Machine Paid Progressive Payout*. The Player Terminal must have a meter that accumulates the total value of credits paid as a result of progressive awards paid directly

by the terminal. This meter does not include awards paid as a result of an external bonusing system;

y) Games Played. The Player Terminal must have meters that accumulates the number of games played:
   i. Since power reset;
   ii. Since external door close; and
   iii. Since game initialization (NV memory clear);

z) External Doors. The Player Terminal must have meters that accumulates the number of times the any external cabinet door that allows access to the locked logic area or currency compartment which was opened since the last NV memory clear, provided power is supplied to the terminal;

aa) Stacker Door. The Player Terminal must have a meter that accumulates the number of times the stacker door has been opened since the last NV memory clear provided power is supplied to the terminal; and

bb) Progressive Occurrence. The Player Terminal must have a meter that accumulates the number of times each progressive meter is activated. See also *GLI-12 Progressive Gaming Devices in Casinos*. (The above rule shall be interpreted as requiring that the controller, whether that is the Player Terminal itself, or an external progressive controller, when configured for progressive functionality, shall provide for this occurrence meter for each progressive level offered.)

2.14.8 Paytable Specific Meters. In addition to the one set of master electronic accounting meters required above, each individual game available for play shall have the paytable meters "Credits Bet" (i.e., coin in) and "Credits Won" (i.e., coin out) in either credits or dollars/cents. Even if a double up or gamble game is lost, the initial win amount, and not credits bet amount, shall be recorded in the game-specific meters.

2.14.9 Double Up or Gamble Meters. For each type of double-up or gamble feature offered, there shall be sufficient meters to determine the feature's actual return percentage, which shall increment accurately every time a double-up or gamble play concludes, including all amounts wagered and won during interim plays. These meters shall reflect amount wagered and amount

won. If the Player Terminal does not supply accounting for the double-up or gamble information, the feature must provide for the ability to be disabled.

2.15 Tokenization – Residual Credits

2.15.1 General Statement. If residual credits exist, the manufacturer may provide a residual credit removal feature or any allowable cashout method to remove the residual credits or return the Player Terminal to normal game play (i.e., leave the residual credits on the player's credit meter for betting). In addition:

a) Residual credits bet on the residual credit removal play shall be added to the coin-in meter. Residual credits won as a result of the residual credit removal play shall be added to the coin-out meter;

b) If the residual credit removal play is won, the value of the win shall either:
   i. Increment the player's credit meter; or
   ii. Be automatically dispensed, and the value of the coin(s) added to the coin-out meter;

c) All other appropriate Player Terminal meters shall be appropriately updated;

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

e) If the residual credits are cashed out rather than wagered, the Player Terminal shall update the relevant meters (e.g., cancelled credit);

f) The residual credit removal play feature shall return at least seventy-five percent (75%) to the player over the life of the game (or a specified return percentage that is consistent with jurisdictional regulations);

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

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

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

j) If the residual credit removal play is offered on a multi-game Player Terminal, 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

k) 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.

NOTE: The above-stated metering requirements shall not preclude the use of thin client technology. In this case, metering shall be satisfied by either the Player Terminal or the Client Server System, as defined in GLI-21.

CHAPTER 3

3.0 Central System Requirements

3.1 System Functions

3.1.1 General Statement. The Central System shall be dedicated primarily to Electronic Ticket system functions related to the creation of Electronic Tickets and their creation, randomization, storage, and transmittal to the Player Terminal(s). It shall also be capable of generating the data necessary to provide the reports required within this section. The Central System shall be operationally independent from the Player Terminal(s).

NOTE: If applicable, additional Client Server System requirements shall be satisfied, as found in GLI-21 Client-Server Systems.

3.1.2 Other Features used with Finite Systems. Finite Systems may allow other functions such as Progressives, Cashless Gaming, Bonusing, Promotions and other gaming management or marketing functions. These systems shall not interfere with, or in any way affect, the outcome of any Finite Game being played. For Finite Systems that allow for 'other functions,' the Player Terminal(s) shall meet the rules governed for each feature, in addition to this standard.

3.1.3 Randomization. The Central System shall utilize randomizing procedures in the creation of the Game Sets for Electronic Tickets or Game Outcomes. The randomizing procedures shall be in accordance with the rules established within the Section entitled 'Mechanical and Electro-Mechanical Random Number Generator (RNG) Requirements' of GLI-11 Gaming Devices in Casinos, with the exception of the section relevant to 'Mechanical-Based RNG Games'.

3.1.4 Game Set Requirements. Each Game Set shall meet the following minimum requirements:

a) Each Game Set shall be made up of a finite number of Electronic Tickets;
b) All Electronic Tickets in a particular Game Set shall be of the same purchase price;
c) Each Game Set shall be assigned a unique serial number;
d) Each Electronic Ticket shall have a specific outcome and prize level associated with it;
e) After randomization, Game Sets may be broken into Game Subsets of equal size. If Game Subsets are used, they shall be assigned a unique serial number.

3.1.5 Data Required to be Available Prior to Commencement of an Electronic Ticket Game Set. The following data shall be available prior to the commencement of an Electronic Ticket Game Set and shall be maintained and be viewable both electronically and if requested, by printed report, upon demand:

a) A unique identifying Game Set serial number;
b) A description of the Game Set sufficient to categorize the Game Set relative to other Game Sets;
c) The number of total Electronic Tickets in the Game Set;
d) The number of Electronic Ticket Game Subsets to be created from the Game Set, and the number of Electronic Tickets in each Set;
e) The payout percentage of the entire Game Set;
f) The overall payback percentage for the Game Set and the number of Electronic Tickets at each award amount; and
g) The purchase price per Electronic Ticket assigned to the Game Set.

3.1.6 Dispensing of Electronic Tickets. The Central System shall dispense, upon request from a Player Terminal, an Electronic Ticket or Game Outcome. All finite games must be played without replacement. Once dispensed, such ticket or outcome must not be re-used until the Game Set is replenished.

3.1.7 Data Required to be Available Following the Completion of an Electronic Ticket Game Set. The following data shall be available, maintained and viewable both electronically and if requested, by printed report, upon demand:

a) The Game Set and Game Subsets serial numbers;
b) The unique name of the Game Set;
c) The total number of Electronic Tickets unsold, if the game is removed from play;
d) The total number of Electronic Tickets purchased;
e) The time and date that the Electronic Ticket was completed or removed from play;
f) The final payout percentage of the Game Set; and
g) The price per Electronic Ticket.

3.1.8 Game Set Auditing. In order to provide maximum game integrity, no audit or other determination of the status of any Game Set or any Game Subset, including but not limited to a determination of the prizes won or prizes remaining to be won, shall be conducted by anyone while a Game Set or Game Subset is in play without causing termination of the entire Game Set / Game Subset. Only upon Game Set termination shall the details of the associated Game Set and Game Subsets be revealed to the individual(s) performing the audit.

3.1.9 Game Set Definition. All finite Game Set definition files must contain the following information:

a) Game Set ID;
b) Game Set type;
c) Game Set Version;
d) Manufacturer;
e) Game name;
f) Paytable ID;
g) Purchase price per Electronic Ticket;
h) Game Subset size definition;
i) Total number of Game Subsets; and

j) Prize values with an associated index and frequency associated with how many of that particular prize exist.

3.2 Central System Security Requirements

3.2.1 General Statement. The Central System computer(s) must be in a locked, secure enclosure that utilizes key(s) that are controlled by the regulatory body.

3.2.2 Security from Alteration, Tampering, or Unauthorized Access. The Central System shall provide a secure physical and electronic means, for securing the Game Sets against alteration, tampering, or unauthorized access. The Central System shall provide a means for terminating the Game Set if unopened ticket information has been accessed, or at the discretion of the regulatory body.

3.2.3 Data Alteration. The Central System shall not permit the alteration of any accounting or significant event log information that was properly communicated from the Player Terminal without supervised access controls. In the event financial data is changed, an automated 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).

3.2.4 Storage Medium Backup.

a) The Central System computer(s) shall have a medium for securely storing Electronic Ticket Game Sets on the computer(s) which shall be mirrored in real time by a backup medium. The Central System computer(s) shall also provide a means for storing duplicates of the Game Sets, already transmitted to the Player Terminals, so as to reflect,

on an ongoing basis, changes in the transmitted Game Sets as they occur. In addition, duplicates of the Game Sets, as created and stored on the Central System computer, shall be stored within a secure enclosure in the gaming facility.

b) All storage shall be through an error checking, nonvolatile physical medium, or an equivalent architectural implementation, so that should the primary storage medium fail, the functions of the Central System computer and the process of auditing those functions can continue with no critical data loss.

c) The database shall be stored on redundant media so that no single failure of any portion of the system would cause the loss or corruption of data.

3.2.5 Recovery Requirements. In the event of a catastrophic failure when the Central System can not be restarted in any other way, it shall be possible to reload the Central 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 employee file, progressive set-up, etc.

3.2.6 Secure Connections and Communications; DES or Equivalent Data Encryption. Connections between all components of the Central System shall only be through the use of secure communication protocols which are designed to prevent unauthorized access or tampering, employing Data Encryption Standards (DES) or equivalent encryption with changeable seeds or algorithms. More specifically, secure connections and encryption shall be utilized between the interface component and the system. This same level of security is not required between the Player Terminal and the interface component when they are housed within the same physical cabinet or enclosure.

a) All data communication shall incorporate an error detection and correction scheme to ensure the data is transmitted and received accurately.

b) The system shall be capable of detecting and displaying certain conditions (see below).

c) These conditions shall be recorded on an error log that may be displayed or printed on demand, and shall archive the conditions for a minimum of 90 days. The conditions include but are not limited to:
   i) Power reset or failure of a Player Terminal or any component of the on-line data system.
   ii) Communication loss between a Player Terminal and any component of the on-line data system.

d) The system shall not permit the alteration of any accounting or event log information that was properly communicated from the Player Terminal unless documented, secure access controls are provided.

3.2.7 Password Access.

a) The Operating System of the Central System must provide comprehensive password security or other secure means of ensuring data integrity and enforcing user permissions;

b) It is required that all programs and important data files must only be accessible via the entry of a password that will be known only to authorized personnel;

c) The storage of passwords and PINs must be in an encrypted, non-reversible form;

d) A program must be available that will list all registered users on the Central System including their privilege level; and

e) The Personal Identification Number (PIN) must have a length of at least six (6) American Standard Code for Information Interchange (ASCII) characters.

3.2.8 System Log-On.

a) The Operating System and/or any Central System-related control program must have a password sign-on with two (2) level codes comprising the personal identification code and a personal special password;

b) The Personal Identification Number (PIN) must have a length of at least six (6) American Standard Code for Information Interchange (ASCII) characters; and

c) It is required that the personal special password have a minimum character length of six

(6), which should include at least one (1) non-alphabetic character.

3.2.9 Security Level and Access Restrictions.

a) The Operating System must have multiple security access levels to control and restrict different classes of access to the Central System; and

b) The Central System access accounts must be unique when assigned to the authorized personnel and shared accounts amongst authorized personnel must not be allowed.

3.2.10 Multiple Log-on at System Management Level (i.e. Primary vs. Secondary Operation).

a) The Operating System must have the capability to control the potential data corruption that can be created by multiple log-ons at the system management level, by the system management personnel, from which the same critical data file can be accessed and changed;

b) The Operating System must specify which of the access levels allow for multiple sign-ons by different users and which of the access levels do not allow for multiple sign-ons, and if multiple sign-ons are possible what restrictions, if any, exist; and

c) If the Central System does not provide adequate control, a comprehensive procedural control document must be drafted to complement this system deficiency in order to assist and enforce a proper normal system operation.

3.2.11 Network Requirements.

a) Where the Central System or components are linked with one another in a local network for function sharing 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.

b) Dedicated and protected network connections prohibiting unauthorized access, may allow two or more Central Systems to share information. Game Set details and other information prohibited from being viewed, as outlined in other sections of this standard, shall not be available or transmitted between the connected systems or facilities.

3.3 Electronic Accounting and Reporting

3.3.1 General Statement. One or more Electronic Accounting System shall be required to perform reporting and other functions in support of the Finite Game activities described in this section. These systems may communicate with the other computers described elsewhere in this document, utilizing the protocol standards agreed upon by participating suppliers. The Electronic Accounting System shall not interfere with the outcome of any gaming functions.

3.3.2 Revenue Reporting Requirements. The following reporting capabilities must be provided by the Electronic Accounting System:

a) Player Terminal Revenue Report. A revenue report for each Player Terminal must be made and maintained on a confidential and secure basis which, at a minimum of a daily and monthly basis, provides:
   i) The total amount won per prize level for each Electronic Ticket Game Set and the total amount won per Game Set per Player Terminal;
   ii) The amount wagered per Game type per Player Terminal;
   iii) The amount of money (cash in) deposited into each Player Terminal; and
   iv) The amount of money removed from each Player Terminal (coin, cash, or ticket/voucher out).

b) Electronic Ticket Game Set Report (for Game Sets in play). An Electronic Ticket Game Set report must be made and maintained on a confidential and secure basis which, on a minimum of a daily and monthly basis, provides as to each Electronic Ticket *in play* which shall be maintained and viewable both electronically and if requested, by printed report, upon demand:
   i) All Games in play without revealing the unused Electronic Tickets and/or prizes remaining in the Game Set.

c) Electronic Ticket Game Set Report (for completed Game Sets). An Electronic Ticket Game Set report must be made and maintained on a confidential and secure basis which,

on a minimum of a daily and monthly basis, provides as to each *completed* Electronic Ticket Game Set which shall be maintained and viewable both electronically and if requested, by printed report, upon demand:

i) All completed Game Sets; See also section entitled "Data Required to be Available Following the Completion of an Electronic Ticket Game Set", earlier in this standard.

ii) The total number of Electronic Tickets sold/unsold in each completed Game Set;

iii) The total prizes paid/remaining to be paid in each completed Game Set;

iv) The Game Set serial numbers;

v) The total number of Electronic Tickets at each prize or other game category level, that were dispensed by the Central System to Player Terminals, and the total number of Electronic Tickets in each such category that were sold at each Player Terminal; and

vi) The final payout percentage of the completed Game Set.

d) A report will be required for all prizes that exceed the threshold that triggers additional procedures to be followed for the purposes of compliance with federal tax reporting requirements. At a minimum, on a daily and monthly basis, the report shall provide the following information per Player Terminal:

i) The date and time won; and

ii) Amount of all prizes.

e) Liability reports will be required on a periodic basis, as specified by the regulatory body. They should provide a summary of the outstanding funds which carry from business day to business day. At a minimum, they must include:

i) Amount of prizes which were awarded, but have not yet been claimed;

ii) Detail of prizes for which redemption period expired during this reporting period;

iii) Unredeemed Game Plays and Winnings; and

iv) Expired Game Plays and Winnings.

3.4 Verification Data and Security Checks

3.4.1 Verification Data and Security Checks. The Central System may be used to record the data used to verify game play and to configure and perform security checks on Player Terminals, provided such functions do not affect the security, integrity or outcome of such games.

3.4.2 Verification of System Software. Central System software components/modules shall be verifiable by a secure means at the system level denoting Program ID and Version. The Central System shall have the ability to allow for an independent integrity check of the components/modules from an outside source and is required for all control programs that may affect the integrity of the Central System. This must be accomplished by being authenticated by a third-party device, which may be embedded within the Central System software (see note below) or having an interface port for a third-party device to authenticate the media. This integrity check will provide a means for field verification of the Central System components/modules to identify and validate the programs/files. The test laboratory, prior to system approval, shall approve the integrity check method.

NOTE: If the authentication program is contained within the Central System software, the manufacturer must receive written approval from the test laboratory prior to submission.

3.5 Random Number Generator

3.5.1 Random Number Generators. Any random number generation used in connection with the Central System must be by use of a microprocessor and random number generation program that meets the following random selection tests:

a) Chi-Square Analysis. Each card, symbol, number, or position which is wholly or partially determinative of the outcome of the game satisfies the 99 percent confidence limit using the standard chi-square analysis.

b) Runs Test. Each card, symbol, number, or position does not as a significant statistic produce predictable patterns of game elements or occurrences. Each card symbol, number, or position will be considered random if it meets the 99 percent confidence level with regard to the "runs test" or any generally accepted pattern testing statistic.

c) Correlation Analysis. Each card, symbol, number, or position is independently chosen without regard to any other card, symbol, number or position, drawn within that game play. Each card, symbol, number, or position is considered random if it meets the 99 percent confidence level using standard correlation analysis.

d) Serial Correlation Analysis. Each card, symbol, number, or position is independently chosen without reference to the same card, number, or position in the previous game. Each card, number, or position is considered random if it meets the 99 percent confidence level using standard serial correlation analysis.

3.6 Communications

3.6.1 Secure Communications.

a) All communications that initiate a Player Terminal pay command shall employ some form of encryption that has been approved by the regulatory body.

b) All data communication shall incorporate an error detection and correction scheme approved by the regulatory body to ensure the data is transmitted and received accurately.

c) The Central System shall be capable of detecting and displaying certain conditions. These conditions shall be recorded on an error log that may be displayed or printed on demand, and shall archive the conditions for a minimum of 90 days. The conditions include but are not limited to:

   i) Power reset or failure of a Player Terminal or any component of the Central System.

   ii) Communication loss between a Player Terminal and any component of the Central System.

3.6.2 Encryption Keys Minimum Width. The minimum width (size) for encryption keys is 112 bits for symmetric algorithms and 1024 bits for public keys.

3.6.3 Encryption Key Handling. There must be a secure method implemented for changing the current encryption key set. It is not acceptable to only use the current key set to "encrypt" the next set. An example of an acceptable method of exchanging keys is the use of public key encryption techniques to transfer new key sets.

3.6.4 Encryption Key Storage. There must be a secure method in place for the storage of any encryption keys. Encryption keys must not be stored without being encrypted themselves.

3.6.5 Significant Events. The following significant events must be collected from the Player Terminal and communicated to the Central System for storage:

a) Power Resets or power failure;
b) Hand pay Conditions (amount needs to be sent to the system) (if applicable):
    i) Player Terminal Jackpot (An award in excess of the single win limit of the Player Terminal);
c) Door Openings (any external door, that accesses a critical area, on the Player Terminal). Door switches (discrete inputs to the interface element) are acceptable if their operation does not result in redundant or confusing messaging.
d) Bill (Item) Validator Errors ('i' and 'ii' should be sent as a unique message, if supported by the communication protocol):
    i) Stacker full (if supported); and
    ii) Bill (item) jam.
e) Printer Errors:
    i) Printer empty/paper low; and
    ii) Printer disconnect/failure.
f) Any other significant events as defined by the protocol employed by the Central System.

3.6.6 Priority Events. The following significant events must be communicated to the Central System where a mechanism must exist for timely notification (it is permissible for the following significant events to be sent to the system as a generic error code, in cases where the Player Terminal is unable to distinguish the specifics of the event):

a) Loss of communication with interface element;
b) Loss of communication with Player Terminal;
c) Memory corruption of the interface element, if storing critical information; and
d) NV Memory corruption of the Player Terminal.

3.7 Ticket/Voucher Validation System Requirements

3.7.1 General Statement. A ticket/voucher validation system may be entirely integrated into a Central System or exist as an entirely separate entity. Ticket/voucher validation systems are generally classified into two types: bi-directional ticket/voucher systems that allow terminals to print and redeem ticket/vouchers (TITO) and ticket/voucher out (TO) only systems that allow terminals to print ticket/vouchers but do not allow ticket/voucher redemption.

3.7.2 Payment by Ticket/Voucher Printer. Payment by ticket/voucher printer as a method of redeeming unused credits and/or winnings on a Player Terminal is only permissible when the terminal is linked to an approved validation system or Central System that allows validation of the printed ticket/voucher. Validation information shall come from the validation system or Central System using a secure communication protocol.

3.7.3 Ticket/Voucher Information Used by the Player Terminal While Communicating to a Validation System. The ticket/voucher validation system must be able to communicate the following ticket/voucher data to the Electronic Ticket device to print on the ticket/voucher.

a) Casino Name/Site Identifier (It is permissible for this information to be contained on the ticket stock itself);

b) Player Terminal number (or cashier/change booth location number, if ticket/voucher creation outside of the Player Terminal is supported);

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

d) Alpha and numeric dollar amount of the ticket/voucher;

e) Ticket/voucher sequence number;

f) Validation number (including a copy of the validation number on the leading edge of the ticket/voucher);

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

h) Type of transaction or other method or differentiating ticket/voucher types; (assuming multiple ticket/voucher types are available) Additionally, it is strongly recommended that whenever the ticket/voucher type is itself a non-cashable item and/or just a receipt, that the ticket explicitly express that it has "no cash value";

i) Indication of an expiration period from date of issue, or date and time the ticket/voucher will expire (24hr format which is understood by the local date/time format). It is permissible for this information to be contained on the ticket stock itself. (e.g. "Expires in One Year"); and

j) If offline voucher issuance is supported, an offline authentication identifier must, at-a-minimum, be printed on the immediate next line following the leading edge validation number, that in no way overwrites, or otherwise compromises, the printing of the validation number on the ticket. If offline voucher issuance is supported, an offline authentication identifier must, at a minimum, be printed on the immediate next line following the leading edge validation number that in no way overwrites, or otherwise compromises, the printing of the validation number on the ticket (not required for ticket/vouchers that are non-redeemable at a Player Terminal). The offline authentication identifier must be derived by a hash, or other secure encryption method of at least 128 bits, that will uniquely identify the voucher, verify that the redeeming system was also the issuing system, and validate the amount of the voucher. For cases where a suitable authentication identifier is not printed on the voucher, the gaming device must print at most one wagering instrument after the gaming device to system communications have been lost.

NOTE: Some of the above-listed information may also be part of the validation number or barcode. Multiple barcodes are allowed and may represent more than just the validation number.

3.7.4 System Ticket/Voucher Records.

a) The validation system must retrieve the ticket/voucher information correctly based on the secure communication protocol implemented, and store the ticket/voucher information into a database.
b) The ticket/voucher record on the host system must contain at a minimum the following ticket/voucher information:
    i) Validation number;
    ii) Date and time the Player Terminal printed the ticket/voucher (24 hr format which is understood by the local date/time format);
    iii) Type of transaction or other method of differentiating ticket/voucher types (assuming multiple ticket/voucher types are available;
    iv) Numeric value of ticket/voucher in dollars and cents;
    v) Status of ticket/voucher (i.e., valid, unredeemed, pending, void, invalid, redemption in progress, redeemed, etc.);
    vi) Date and time the ticket/voucher will expire (24 hr format which is understood by the local date/time format or expiration period from date of issuance); and
    vii) Player Terminal /machine number that identifies where the ticket/voucher was issued from.

3.7.5 Ticket/Voucher Printing During Loss of Communication with Validation System. For validation systems that communicate to an Electronic Ticket device through an SMIB (Smart Machine Interface Board), if any links between the SMIB and the back-end database go down, the SMIB must:

a) Not respond to the validation request from the terminal and stop ticket/voucher printing, or

b) Prevent the Player Terminal from further ticket/voucher issuance, or

c) Not read or store any further ticket/voucher information generated by the terminal.

NOTE: A maximum of 1 (one) off-line ticket/vouchers directly after loss of communication is acceptable, in cases where the interface element has already been 'seeded' by the system, provided the ticket/voucher issuance information is sent immediately, when communication is re-established.

3.7.6 Database and Validation Component Security. 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/voucher information shall not have any options or method that may compromise ticket/voucher information. Any device that holds ticket/voucher 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.

3.8 Ticket/Voucher Issuance and Redemption

3.8.1 Ticket/Voucher Issuance. A ticket/voucher can be generated at a Player Terminal through an internal printer. Ticket/vouchers that reflect partial credits may be issued automatically from a Player Terminal. Additionally, cashier/change booth issuance is permitted if supported by the validation system.

3.8.2 Offline Ticket/Voucher Issuance. The Player Terminal must meet the following minimum set of requirements to incorporate the ability to issue offline vouchers after a loss of communication has been identified by the terminal.

a) Rules for Issuance. The Player Terminal shall not issue more offline vouchers than has the ability to retain and display in the terminal maintained ticket out log.

b) Request for Re-Seeding. The Player Terminal shall not request validation numbers and seed, key, etc. values used in the issuance of vouchers until all outstanding offline voucher information has been fully communicated to the ticket/voucher validation system.

c) Rules for Re-Seeding. The Player Terminal shall request a new set of validation numbers and seed, key, etc. values used in the issuance of online/offline voucher if the current list of validation numbers and seed, key, etc. values have the possibility of being compromised which include but are not limited to the following cases:
   i. After power has been recycled, and/or
   ii. Upon exit of a main door open condition.

d) The values for the seed, key, etc. must never be viewable through any display supported by the Player Terminal. Additionally, validation numbers must always be masked when viewable through any display supported by the terminal such that only the last 4 digits of the validation number are visible.

3.8.3 Online Ticket/Voucher Redemption. Ticket/vouchers may be inserted in any Player Terminal participating in the validation system providing that no credits are issued to the terminal prior to confirmation of ticket/voucher validity.

3.8.4 Offline Ticket/Voucher Redemption. The offline ticket/voucher redemption may be validated as an internal control process at the specific Player Terminal that issued the ticket/voucher. A manual handpay may be conducted for the offline ticket/voucher value.

3.9 Ticket/Voucher Reporting Requirements

3.9.1 Ticket/Voucher Reporting Requirements. The following reports shall be generated at a minimum and reconciled with all validated/redeemed ticket/vouchers:

a) Ticket/voucher Issuance Report;

b) Ticket/voucher Redemption Report;

c) Ticket/Voucher Liability Report;

d) Transaction Detail Report must be available from the validation system that shows all ticket/vouchers generated by an Electronic Ticket device and all ticket/vouchers redeemed by the validation terminal; and

e) Cashier Report, which is to detail individual ticket/vouchers, the sum of the ticket/vouchers paid by the redemption area.