STANDARD SERIES

GLI-20:

Kiosks

Version: 1.5

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.

This Page Intentionally Left Blank

Table of Contents

This Page Intentionally Left Blank

CHAPTER 1
1.0 OVERVIEW - KIOSKS

1.1 Introduction

1.1.1 Kiosks Defined. Kiosks are patron interface units that may be used to perform various tasks including, but not limited to:

a) Ticket/Voucher/Coupon Redemption - Kiosks are usually interfaced to some type of monitoring or control system that will play a role in the critical functions of the kiosk. Gaming Devices that have the option of issuing payments via ticket/voucher printers are customarily interfaced to a Validation System as explained in GLI-11 and in GLI-13. When a ticket/voucher is redeemed for cash, the ticket/voucher on the Validation System must be updated to reflect a 'Redeemed' status. When using a Kiosk as the method of redemption, the Kiosk shall read the ticket/voucher and notify the Validation System of all required validation information. The system is then to determine if the ticket/voucher is valid and transmit to the Kiosk the amount to be paid or instruct the kiosk to reject the ticket/voucher. For valid ticket/vouchers, payment is made to the patrons from various denominations, coin and currency payment mechanisms.

b) Bill Breaking – Bill Breaking is the act of making change. A patron may wish to insert a bill for any combination of change. It may include an insertion of a large denomination bill for the issuance of smaller denomination bills. It may also include the insertion of small denomination bills for the issuance of coin.

c) Ticket Issuance - Ticket issuance kiosks that issue tickets/vouchers via ticket/voucher printers must be interfaced to a validation system. When a ticket/voucher is printed from the kiosk, the ticket/voucher on the validation system must be updated to reflect a 'Pending' status. The ticket issuance kiosk must receive all its validation information from the ticket validation system. The ticket validation system must ensure that the correct information is sent to the ticket issuance kiosk and the kiosk must validate the

incoming message packets through an error checking mechanism before printing a ticket. When the ticket/voucher printed by the kiosk is redeemed at a gaming device, cashiers cage or kiosk, the system must change the 'Pending' status of the ticket/voucher to 'Redeemed'.

d) Promotional Point Redemption - Promotional Point Redemption defines the process of a patron redeeming their promotional player points at the kiosk for cash or a ticket/voucher. The kiosk in this case is being used as an alternative to the current process of the player approaching the casino cage or player services desk to redeem their points. The kiosk in this case shall only be interfaced to an approved promotional system/gateway. This standard will only address the use of kiosks when redeeming player points for cash or ticket/voucher. This standard will not address the use of kiosks for redemption of player points for casino merchandise and/or services.

e) Information Reporting – The kiosk can be used to display marketing information for customers. This feature is not covered by this standard as it does not affect the integrity of Kiosk Security and/or Accounting.

1.1.2 Phases of Certification. The certification of a Kiosk shall be based on laboratory testing, where the laboratory will test the integrity of the kiosk in conjunction with each compatible system(s) along with compliance with to this document.

1.1.3 Document History. This document is an essay from many standards documents from around the world. Some GLI has written; some, such as the Australian and New Zealand National Standard, were written by Industry Regulators with input from test laboratories and device manufacturers. We have taken each of the standards' documents, merged each of the unique rules together, eliminating some rules and updating others, in order to reflect both the change in technology and the purpose of maintaining an objective, factual standard. We have listed below, and given credit to, agencies whose documents we reviewed prior to writing this Standard. It is the policy of **Gaming Laboratories International, LLC** to update this document as often as possible to reflect changes in technology, testing methods, or cheating methods. This document will be distributed without charge to all those who request it. It may be obtained by downloading it from our website at www.gaminglabs.com or by writing to us at:

Gaming Laboratories International, LLC
600 Airport Road
Lakewood, NJ 08701
(732) 942-3999 Tel
(732) 942-0043 Fax

* *Please note a comprehensive revision history of this document is available upon request*

1.2 Purpose of Technical Standard

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

a) To eliminate subjective criteria in analyzing and certifying Kiosk operations;

b) To only test those criteria which impact the credibility and integrity of a Kiosk from both the revenue collection and security perspective.

c) To create a standard that will ensure that Kiosks in casinos 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 jurisdiction to set public policy with respect to Kiosks;

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 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.

1.2.2 No Limitation of Technology. One should be cautioned that this document 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 Other Documents That May Apply

1.3.1 General Statement. This standard covers the minimal requirements for Kiosks. The following other standards may apply:

a) GLI-11 Gaming Devices in Casinos
b) GLI-13 On-line Monitoring and Control System (MCS) and Validation Systems in Casinos
c) GLI-16 Cashless Systems in Casinos
d) GLI-18 Promotional Systems in
e) Individual Jurisdictional Specific Minimum Internal Control Procedures.

CHAPTER 2
2.0 KIOSK HARDWARE REQUIREMENTS

2.1 Terminal Requirements

2.1.1 Kiosk Terminal Security. The main door, that must be locked, shall be manufactured of materials that are suitable for allowing only legitimate access to the inside of the kiosk terminal (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 Kiosk, and shall leave evidence of tampering if such an entry is made.

2.1.2 Kiosk Terminal Wiring. The Kiosk shall be designed so that power and data cables into and out of the kiosk can be routed, so that they are not accessible to the general public. This is for kiosk 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 kiosk terminal. Wireless Kiosks would need to comply with individual jurisdictional wireless security requirements.

NOTE: The Laboratory will make no determination as to whether the Kiosk installation conforms to local electrical codes, standards and practices

2.1.3 On/Off Switch. An on/off switch that controls the electrical current shall be located in a place which is readily accessible within the interior of the kiosk so that power cannot be disconnected from outside of the kiosk using the on/off switch. The on/off positions of the switch shall be labeled.

2.1.4 Switches and Jumpers. If the Kiosk contains 'Switches and/or Jumpers', all switches or jumpers shall be fully documented for evaluation by the test laboratory

2.1.5 Kiosk Terminal Identification. The Kiosk must 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 must include the following information:

a) The Manufacturer;
b) A Unique Serial Number;
c) A Kiosk Model Number; and
d) The Date of Manufacture.

2.1.6 Patron Safety. Electrical and mechanical parts and design principals of the kiosk terminal must not subject a patron to any physical hazards. The gaming test laboratory shall not make any finding with regard to Safety and Electromagnetic Compatibility (EMC) testing, as this is the responsibility of the manufacturer of the devices or those that purchase the devices. Such Safety and EMC testing may be required under separate statute, regulation, law or Act and should be researched accordingly, by those parties who manufacture or purchase said devices. The gaming test laboratory shall not test for, be liable for, nor make a finding relating to these matters.

2.1.7 Kiosk Integrity. The Laboratory will perform certain tests to determine whether or not outside influences affect performance or create cheating opportunities. This certification applies exclusively to tests conducted using current and retrospective methodology developed by Gaming Laboratories International, LLC (GLI). During the course of testing, GLI inspects for marks or symbols indicating that a device has undergone product safety compliance testing. Gaming Laboratories International, LLC also performs, where possible, a cursory review of submissions and information contained therein related to Electromagnetic Interference (EMI), Radio Frequency Interference (RFI), Magnetic Interference, Liquid Spills, Power Fluctuations and Environmental conditions. Electrostatic Discharge Testing is intended only to simulate techniques observed in the field being used to attempt to disrupt the integrity of the kiosk. Compliance to any such regulations related to the aforementioned testing is the sole

responsibility of the device manufacturer. Gaming Laboratories International, LLC claims no liability and makes no representations with respect to such non-gaming testing.

A Kiosk shall be able to withstand the following tests, resuming operation without operator intervention:

a) Electro-static Interference. Protection against static discharges requires that the Kiosk's conductive cabinets be earthed in such a way that static discharge energy shall not permanently damage or permanently inhibit the normal operation of the electronics or other components within the kiosk. Kiosks may exhibit temporary disruption when subjected to a significant electro-static discharge greater than human body discharge, but they shall exhibit the capacity to recover and complete any interrupted function without loss or corruption of any control or critical data information associated with the kiosk. The tests will be conducted with a severity level of a maximum of 27KV air discharge;

NOTE: For commercial components involved in functions covered by this standard that are affected (e.g. a PC monitor), there must be a method to determine the state the Kiosk was in if any of the components fail from static discharge.

2.1.8 Tower Light. A kiosk involved in functions covered by this standard shall have a light located conspicuously on its top, that automatically illuminates when an error condition has occurred or a 'Call Attendant' (if applicable) has been initiated by the patron. This requirement may be substituted for an alternate means that alerts casino staff of error conditions and patron seeking assistance occurrences.

NOTE: The Laboratory will make no determination as to tower light color or flash sequence. Furthermore, alternative means to alert appropriate personnel will be considered on a case-by-case basis.

2.1.9 Requirements for External Doors/External Compartments. The interior of the kiosk cabinet should not be accessible when all doors are closed and locked. Doors shall be

manufactured of materials that are suitable for allowing only legitimate access to the inside of the kiosk 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 kiosk cabinet and shall leave evidence of tampering if such an entry is made).

2.1.10 The Kiosk Logic Door and Logic Area. It is recommended that the Kiosk utilize a logic area which is a separately locked cabinet area (with its own locked door) which houses electronic components that have the potential to significantly influence the operation of the kiosk. There may be more that one (1) such logic area in a kiosk.

2.1.11 Electronic Components. Electronic components that are recommended to be housed in one (1) or more logic areas are:

a) A CPU and any program storage device that contains software that may affect the integrity of the kiosk, including, but not limited to, accounting, system communication, and peripheral firmware devices involved in, or which significantly influence the intended operation of a kiosk or accounting, revenue, or security. Any exceptions 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; and
c) The NV memory back-up device, if applicable, is also recommended to be kept within a locked logic area.

2.1.12 Coin/Token and Currency Compartments. It is recommended that the coin or token and currency compartments be locked separately from the main kiosk cabinet area. It is also recommended that access to the currency storage area be secured via separate key locks, and the kiosk be fitted with sensors that indicate door open/close or stacker receptacle removed, provided power is supplied to the kiosk. If the kiosk is interfaced with a monitoring system; it is recommended that these alerts be sent to the system when possible.

2.1.13 Video Monitors/Touch Screens. Video monitor touch screens shall meet the following rules::

a) A touch screen (if applicable) shall be accurate and once calibrated shall maintain that accuracy for at least the manufacturer's recommended maintenance period;
b) A touch screen (if applicable) should be able to be re-calibrated without access to the kiosk cabinet other than opening the main door; and
c) There shall be no hidden or undocumented buttons/touch points (if applicable) anywhere on the screen that negatively affect and/or impact the proper operation of the kiosk, except as provided for, by the instructions for kiosk usage for the patron.

2.1.14 Back-up of Memory. The Kiosk shall have the ability to retain data for all critical memory as defined herein and shall be capable of maintaining the accuracy of all information required for thirty (30) days after power is discontinued from the Kiosk.

2.2 Coin Acceptors and Diverters

2.2.1 Diverter. For kiosks 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 after the state change, without causing a disruption of coin flow or creating a coin jam. Hopper-less kiosks shall always divert coins to the drop box.

2.2.2 Coin or Token Acceptors. If the kiosk 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) 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 other manipulation that may be deemed as a fraudulent technique.

b) Rapidly Fed Coins: The kiosk shall be capable of handling rapidly fed coins or piggy backed coins so that occurrences of cheating are eliminated;

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

d) Invalid Coins: Coins deemed invalid by the acceptor shall be rejected to the coin tray and shall not be counted as credits;

e) Coin Acceptance Conditions: Acceptance of coins for crediting to the transaction meter shall only be possible when the kiosk is enabled for use. Other states, such as error conditions, including door opens and audit mode shall cause the disabling of the coin acceptor system.

2.3 Bill Validators

2.3.1 ***Bill*. Validators** All paper currency 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 kiosk 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 gaming device. 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 mediums:

a) Each valid bill, coupon, ticket/voucher or other approved note shall register the actual monetary value or the appropriate number of credits received on the kiosk;
b) Credit meter update upon bill insertion. Cash shall only be dispensed when:
    i. The bill or other note has passed the point where it is accepted and stacked; and
    ii. The validator has sent the "irrevocable stacked" message to the kiosk.

2.3.2 Communications. All bill validators shall communicate with the kiosk using a bi-directional protocol.

2.3.3 Factory Set 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 desired acceptance for bills, coupons, ticket/vouchers or other approved notes and their limits;
b) Changing of certified control program media or downloading of certified software;
c) Adjustments of the bill validator for the tolerance level for accepting bills or notes of varying quality should not be allowed externally to the kiosk. 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 acceptance.

2.3.4 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 kiosk 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) It is recommended there be a separately keyed lock to access the stacker area. This keyed lock shall be separate from the main door. In addition, a separately keyed lock shall be required to remove the bills from the stacker.

2.3.5 ***Self Test***. The bill validator device shall perform a self test at each power up. In the event of a self test failure, the bill validator shall automatically disable itself (i.e.: enter bill reject state) until the error state has been cleared.

CHAPTER 3
2.0 SOFTWARE REQUIREMENTS

3.1 Contents of Critical Memory

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

a) All Electronic Meters required in Section 3.6 "Metering" defined by this document; including last bill data and door open metering;
b) Ticket/Voucher Redeemed Log, provided the log is not stored on printed paper within the device; and
c) Software state (the last normal state, last status or tilt status the Kiosk software was in before interruption).

3.1.2 Function of Non-Volatile Memory Reset. Following the initiation of an NV Memory reset procedure (utilizing a certified NV Memory Clear method) the Kiosk software 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 Kiosks that allow for partial NV memory clears, the methodology in doing so must be accurate.

3.1.3 Maintenance of Critical Memory. 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.

NOTE: The "Maintenance of Critical Memory" section 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.

3.1.4 Data Alteration. The Kiosk shall not permit the alteration of any Meter or Error Condition log information without supervised access controls. In the event Meter or Error Condition log data is changed, an audit log 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 Communication

3.2.1 Communication Components. For Ticket or Coupon Issuance and/or Redemption features, the Kiosk must be designed to allow for communication with a Validation System. All communications between the Kiosks and the Validation System must be secured. This network security must be implemented by the casino's Information Technology (IT) department.

3.3 Error Conditions

3.3.1 General Statement. The Kiosk shall be capable of detecting and displaying the following Error Conditions. The Error Condition must illuminate the tower light or sound an audible alarm. The Kiosk shall be able to recover to the state it was in immediately prior to the interruption occurring, including during payment. Error Conditions requiring attendant intervention are denoted by an '*':

a) Power loss or power reset;

b) System and Kiosk not communicating (this may be detected upon ticket insertion/issuance request only)
c) Coin or currency out error*;
d) Coin Hopper or Cash Dispenser empty or timed out *(should not require immediate intervention if alternate method of payment available (e.g. 6 dollar ticket and 5 dollar bill hopper out but, unit could still pay in ones from the 1 dollar hopper));
e) RAM error (critical memory)*;
f) Low RAM battery (if battery external to the RAM itself used)*;
i) Ticket/Voucher-in jam*;
j) Door open (all external doors);
k) Bill acceptor stacker full (this condition should cause the Bill Acceptor to disable itself to no longer accept anything);
l) Bill acceptor door open;
m) Stacker door open or stacker removed; and
n) Printer* errors, where applicable, which would include:
    i. Out of paper/paper low;
    ii. Printer jam/failure; and
    iii. Printer disconnected – which may only be detected when the software tries to print.

NOTE: For Kiosks that use error codes, a description of the kiosk error codes and their meanings shall be affixed on the inside of the Kiosk.

NOTE: If any of the above Error Conditions occur during the acceptance and/or escrowing of a ticket/voucher, the ticket/voucher must be returned to the patron without a status change on the Validation System or, once the Error Condition is cleared, proceed to pay the patron and have a status of 'Redeemed' on the system.

3.4 Program Interruption & Resumption

3.4.1 ***Interruption***. After a program interruption (e.g. processor reset), the kiosk software shall be able to recover to the state it was in immediately prior to the interruption occurring. It is acceptable for the kiosk to return to a completion state provided the history and all credit and accounting meters comprehend a completed state. If a power failure occurs during acceptance of a bill or other note, the bill validator shall give proper credits or return the note, notwithstanding that there may be a small window of time where power may fail and credit may not be given. In this case, the window shall be less than one (1) second

3.4.2 ***Resumption***. On program resumption, the following procedures shall be performed as a minimum requirement.

a) Any communications to an external device shall not begin until the program resumption routine, including self-tests, is completed successfully and
b) Kiosk control programs shall test themselves for possible corruption due to failure of the program storage media. The authentication may use a checksum; however, it is preferred that the Cyclic Redundancy Check (CRC) calculations is used as a minimum (at least 16 bit). Other test methodologies shall be of a certified type; and
c) The integrity of all critical memory shall be checked.

3.5 Transaction Limits

3.5.1 ***General Statement***. Each Kiosk must have the ability to have transaction limits for ticket issuance and also ticket redemption, where applicable. The configuration of the transaction limit must be via a secure means. The local Gaming Commission, if required, will determine the transaction limit.

3.6 Metering

3.6.1 ***General Statement***. The meter information shall only be accessible by an authorized person and must have the ability to be displayed on demand using a secure means. Accounting and Occurrence meters shall be labeled so they can be clearly understood in accordance with their function. All kiosks shall be equipped with a device, mechanism or method for retaining the value of all meter information specified in this section which must be preserved in the event of power loss to the kiosk.

3.6.2 ***Accounting Meters***. Electronic accounting meters shall be at least eight (8) digits in length. If the meter is being used in dollars and cents, at least eight (8) digits must be used for the dollar amount. The meter must roll over to zero upon the next occurrence; any time the meter is eight (8) digits or higher and after 99,999,999 has been reached or any other value that is logical. The following accounting information must be maintained within Critical Memory:

a) A "Total In " Meter(s) that accumulates the total value of all coins, bills, ticket/vouchers and coupons accepted by the device. Separate In meters shall report the value of all tickets redeemed and the value of all bills redeemed and the value of all coins redeemed; and
b) A "Total Out" Meter(s) for payments issued by the machine. Separate 'Out Meters' shall report the value of all coins, bills and tickets dispensed by the machine.
c) A "Hand pay" Meter shall reflect the cumulative amounts paid by an attendant in the event that a ticket cannot be printed

3.6.3 ***Occurrence Meters***. Occurrence meters shall be at least three (3) digits in length and roll over to zero upon the next occurrence, any time the meter is higher than the maximum number of digits. The following occurrence information must be maintained within Critical Memory:

a) A meter that accumulates the number of times the external door(s) was opened;
b) A meter that accumulates the number of times the cash area door(s) was opened;
c) Total number of all notes accepted by the Bill Validator; and

d) A breakdown of each note type accepted by the Bill Acceptor, bills by denomination.

3.7 Verification

3.7.1 Independent Control Program Verification. The kiosk shall have the ability to allow for an independent integrity check of the device's software from an outside source and is required for all control programs that may affect the integrity of the kiosk. This must be accomplished by being authenticated by a third-party device, which may be embedded within the kiosk 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 is can be verified externally. This integrity check will provide a means for field verification of the software to identify and validate the programs. The test laboratory, prior to the kiosk approval, shall evaluate the integrity check method.

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

3.8 Printers

3.8.1 Payment by Ticket/Voucher Printers. If the Kiosk has a printer that is used to make payments, the kiosk may pay the player by issuing a printed ticket/voucher. The printer shall print on a ticket/voucher as indicated in section 3.9.2 titled "Ticket/Voucher Information" and the kiosk shall support the transmission of data to a validation system that records the following information regarding each payout ticket/voucher printed:

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;
c) Date, in any recognized format, indicating the day, month, and year;
d) Kiosk Identification number;

e) Unique validation number.

To further meet this requirement, if the kiosk supports printing duplicate tickets, the kiosk must print only one (1) copy to the patron but have the ability to retain the last twenty-five (25) ticket/voucher-out information* to resolve patron disputes. If the kiosk supports printing single tickets, it shall have the ability to retain the last twenty-five (25) ticket/voucher-out information* electronically. In addition, an approved validation system shall be used to validate the payout ticket/voucher, and the ticket/voucher information on the system shall be retained at least as long as the ticket/voucher is valid at that location. If offline ticket/voucher issuance is supported, the kiosk 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.

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

3.9 Ticket/Voucher Validation

3.9.1 ***Payment by Ticket/Voucher Printer***. Payment by ticket/voucher printer as a method of credit redemption is only permissible when:

a) The Kiosk is linked to a computerized 'Ticket/Voucher Validation System', which allows validation of the printed ticket/voucher. Validation approval or information shall come from the Ticket/Voucher validation system in order to validate ticket/vouchers. Ticket/vouchers may be validated at any location, as long as it meets the standard in this section. Provisions must be made if communication is lost, and validation information cannot be sent to the validation system, thereby requiring the manufacturer to have an alternate method of payment. The validation system must be able to identify duplicate

ticket/vouchers to prevent fraud by reprinting and redeeming a ticket/voucher that was previously issued; or

b) By use of an approved alternative method that includes the ability to identify duplicate ticket/vouchers to prevent fraud by reprinting and redeeming a ticket/voucher that was previously issued.

3.9.2 ***Ticket/Voucher Information***. A ticket/voucher produced by a kiosk shall contain the following printed information at a minimum:

a) Casino Name/Site identifier; (It is permissible for this information to be contained on the ticket stock itself);
b) Kiosk Identification number
c) Date and time (24hr format which is understood by the local date/time format);
d) Alpha and numeric currency 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 of differentiating ticket/voucher types; (assuming multiple ticket/voucher types are available) Additionally, it is strongly recommended that whenever the ticket/voucher type itself is 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 ticket/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/voucher (not required for ticket/vouchers that are non-redeemable at a gaming machine). 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 ticket/voucher, verify that the redeeming system was also the issuing system, and validate the amount of the ticket/voucher. For cases where a suitable authentication identifier is not printed on the ticket/voucher, the kiosk must print at most, one wagering instrument after the kiosk to validation system communication has 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.

3.10 Ticket/Voucher Issuance and Redemption

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

3.10.2 Offline Ticket/Voucher Issuance. If offline ticket/voucher issuance is supported, the kiosk must meet the following minimum set of requirements to incorporate the ability to issue offline ticket/vouchers after a loss of communication has been identified by the kiosk.

a) Rules for Issuance. The kiosk shall not issue more offline ticket/vouchers than it has the ability to retain and display in the kiosk maintained ticket out log.
b) Request for Re-Seeding. The kiosk shall not request validation numbers and seed, key, etc. values used in the issuance of ticket/vouchers until all outstanding offline ticket/voucher information has been fully communicated to the ticket/voucher validation system.
c) Rules for Re-Seeding. The kiosk shall request a new set of validation numbers and seed, key, etc. values used in the issuance of online/offline ticket/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 kiosk. Additionally, validation numbers must always be masked when viewable through any display supported by the kiosk such that only the last 4 digits of the validation number are visible.

3.10.3 Online Ticket/Voucher Redemption. Ticket/vouchers may be inserted in a kiosk participating in the validation system providing that no currency is dispensed by the kiosk prior to confirmation of the ticket/voucher validity.

3.10.4 Offline Ticket/Voucher Redemption If offline ticket/voucher issuance is supported, the offline ticket/voucher redemption may be validated as an internal control process at the specific gaming device or kiosk that issued the ticket/voucher. A manual hand pay may be conducted for the offline ticket/voucher value.