GLI STANDARD SERIES

GLI-20:

STANDARDS FOR KIOSKS

VERSION: 2.0 PUBLIC COMMENT DRAFT

REVISION DATE: APRIL 3, 2019

About This Standard

This technical standard has been produced by **Gaming Laboratories International, LLC (GLI)** for the purpose of providing independent technical analysis and/or certifications to gaming and wagering industry stakeholders indicating the state of compliance for kiosks with the requirements set forth herein.

This document is intended to be used by regulatory bodies, operators, and industry suppliers as a compliance guideline for technologies pertaining to kiosks. This standard is not intended to represent a set of prescriptive requirements that every kiosk must comply with; however, it does establish a technical standard regarding the technologies used to facilitate these operations.

A supplier is expected to submit equipment with a request that it be certified in accordance with this technical standard. Upon completion of testing, GLI provides a certificate of compliance evidencing the certification of the kiosk to this standard.

GLI-20 should be viewed as a living document that provides a level of guidance that will be tailored periodically to align with this developing industry over time as kiosk implementations and operations evolve.

Table of Contents

Chapter 1: Introduction to Kiosks

1.1 Introduction

1.1.1 General Statement

Gaming Laboratories International, LLC (GLI) has been testing gaming equipment since 1989. Over the years, GLI has developed numerous technical standards utilized by jurisdictions all over the world. This document, *GLI-20*, sets forth the technical standards for kiosks.

1.1.2 Document History

This document is a compilation based upon many standards documents from around the world. Some were written by GLI; others were written by industry regulators with input from independent test laboratories and kiosk manufacturers. GLI has taken each of the standards documents and merged the unique rules, eliminated some rules and updated others, to reflect both the change in technology and the purpose of maintaining an objective standard that achieves common regulatory objectives without unnecessarily impeding technological innovation. GLI lists below, and gives credit to, organizations whose documents were reviewed prior to writing this standard. It is the policy of GLI to update this document as often as warranted to reflect changes in technology and/or testing methods. This document will be distributed without charge and may be obtained by downloading it from the GLI website at www.gaminglabs.com or by contacting GLI at:

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

1.2 Acknowledgment of Other Standards Reviewed

1.2.1 General Statement

This technical standard has been developed by reviewing and using portions of the documents from the following organizations. GLI acknowledges and thanks the regulators and other industry participants who have assembled these documents:

a) Nevada Gaming Commission and Gaming Control Board.
b) US Tribal Compacts from Tribal Governments and State Governments including Arizona, Connecticut, Iowa, Kansas, Louisiana, Michigan, Minnesota, Mississippi, North Carolina, North Dakota, Oregon, and Wisconsin.
c) Colorado Division on Gaming.
d) Illinois Gaming Board.
e) Indiana Gaming Commission.
f) Iowa Racing and Gaming Commission.

g) Missouri Gaming Commission.
h) Pennsylvania Gaming Control Board.
i) South Dakota Commission on Gaming.

1.3 Purpose of Technical Standards

1.3.1 General Statement

The purpose of this technical standard is as follows:

a) To eliminate subjective criteria in analyzing and certifying the regulated operations of a kiosk.
b) To test the criteria that 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 are fair, secure, and able to be audited and operated correctly.
d) To distinguish between local public policy and Independent Test Laboratory criteria. It is up to each local jurisdiction to set its own 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 this standard, testing is not directed at health or safety matters. These matters are the responsibility of the manufacturer, purchaser, and operator of the kiosk.
f) To construct a standard that can be easily revised to allow for new technology.
g) To construct a standard that does not specify any particular design, 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 encourage new methods to be developed.

1.3.2 No Limitation of Technology

One should be cautioned that this document must not be read in such a way that limits the use of future technology. This document should not be interpreted to mean that if the technology is not mentioned, then it is not allowed. To the contrary, GLI will review this standard and make changes to incorporate minimum standards for any new and related technology.

1.3.3 Adoption and Observance

This technical standard can be adopted in whole or in part by any regulatory body that wishes to implement a comprehensive set of requirements for kiosks.

1.4 Other Documents That May Apply

1.4.1 Other GLI Standards

This technical standard covers the requirements for the regulated operations of kiosks. Depending on the technology utilized by a kiosk, additional GLI technical standards may also apply.

NOTE: The entire family of GLI Standards is available free of charge at www.gaminglabs.com.

1.5 Definition of a Kiosk

1.5.1 General Statement

Kiosks are player interface units that, as approved by the regulatory body, may be used to perform various regulated operations when interfaced (either directly or through a back-office platform installed externally to the kiosk terminal) with a compatible host system including, but not limited to:

a) Wagering Instrument Issuance and/or Redemption – Kiosks that issue and/or redeem wagering instruments (vouchers and/or coupons) will be interfaced with a host system (validation system) which supports wagering instruments.
b) Player Account Management – Kiosks that allow players to manage their player account (e.g. registration, deposits, withdrawals, etc.) and/or redeem their promotional points for cashable credits will be interfaced with a host system (cashless wagering system, promotional system, etc.) which supports player accounts. This standard will not address the use of kiosks for redemption of promotional points for merchandise and/or services.
c) Event Wagering – Kiosks that allow players to place wagers on events and/or redeem winning wagers must be interfaced with an Event Wagering System.
d) Games of Chance Consumable Purchase and/or Redemption – Kiosks that allow players to purchase consumables for games of chance (raffle tickets, lottery tickets, pull-tabs, bingo cards, keno tickets, etc.) and/or redeem winners will be interfaced with the applicable host system(s).
e) Bill Breaking – Bill Breaking is the act of making change. A player may 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 coins.
f) Information Reporting – The kiosk can be used to display marketing information for players. This feature is not covered by this standard as it does not affect the integrity of kiosk security and/or accounting.

NOTE: Additional requirements beyond this document might apply for kiosks based on their functionality. Please refer to the applicable jurisdictional requirements or GLI Standards for the compatible systems which the kiosk is intended to work with.

Chapter 2: Kiosk Terminal Requirements

2.1 Introduction

2.1.1 General Statement

This chapter sets forth the technical requirements for the key attributes of a kiosk terminal. All proprietary devices developed for kiosks must meet the applicable requirements within this chapter. Unless otherwise directed by the regulatory body, this chapter does not apply to kiosks that solely utilize unaltered commercial off-the-shelf (COTS) components, such as PCs or tablets. For kiosks that utilize modified off-the-shelf (MOTS) components, sections of this chapter will apply only to the modifications made to the components unless otherwise directed by the regulatory body.

2.2 Player Safety

2.2.1 Physical Hazards and Environmental and Electrical Safety Testing

Electrical and mechanical parts and design principles of the kiosk terminal must not subject a player to any physical hazards. The independent test laboratory does not make any findings with regard to Electro-Magnetic Compatibility (EMC) or Radio Frequency Interference (RFI), as that is the responsibility of the manufacturer of the kiosk, or those that purchase the kiosk. Such EMC and RFI testing may be required under separate statute, regulation, law, or act and should be researched accordingly by those parties who manufacture or purchase said kiosk. The independent test laboratory does not test for, is not liable for, nor makes any findings related to these matters. However, during the course of testing, the independent test laboratory may inspect for marks or symbols indicating that a kiosk has undergone product safety or other compliance testing by some other party but that is outside the scope of the requirements defined by this technical standard.

2.3 Environmental Effects on Integrity

2.3.1 General Statement

This section is only applicable for a kiosk terminal which has locally stored critical NV memory and/or installed software which has the potential to influence the regulated operations of the kiosk.

2.3.2 Kiosk Integrity

The independent test laboratory must perform certain tests to determine whether or not an electro-static discharge (ESD) or a power surge impacts the integrity of a kiosk. ESD testing and power surge testing are intended to simulate techniques observed in the field that may be used in an attempt to disrupt the integrity of a kiosk.

2.3.3 ESD Effects

Protection against ESD requires that the kiosk terminal's conductive cabinet be earthed in such a way that static discharge energy shall not permanently damage or permanently impact the normal operation of the electronics or other components within the kiosk terminal. A kiosk may exhibit temporary disruption when subjected to a significant external ESD with a severity level of 15kV air discharge. The kiosk must exhibit a capacity to recover and complete any interrupted operation without loss or corruption of any locally stored control information or critical data following any temporary disruption.

2.3.4 Power Surges

The kiosk terminal must not be adversely affected, other than resets, by surges or dips of ± 10% of the power supply voltage. It is acceptable for the kiosk to reset provided no damage to the equipment or loss or corruption of locally stored data is experienced which cannot be automatically recovered from the back-office platform. Alternatively, the kiosk terminal may be equipped with an Uninterruptible Power Supply (UPS) or battery backup that, when detecting power loss, allows the completion of the current transaction before ceasing operations.

2.4 Basic Hardware Requirements

2.4.1 Identification Information

The kiosk terminal must be identifiable by model number, manufacturer identification, and any other information required by the regulatory body.

2.4.2 On/Off Switch

An on/off switch that controls the electrical current supplied to the kiosk terminal must be located in a secured area of the kiosk terminal. The on/off positions of the switch must be clearly labeled.

2.4.3 Touch Screen Displays

Touch screen displays, if in use by regulated operations of the kiosk, must be accurate, and if required by their design, must support a calibration method to maintain that accuracy; alternatively, the display hardware may support automatic self-calibration.

2.5 Custom and Modified Hardware

2.5.1 General Statement

This section only applies to custom and modified hardware components which have the potential to influence the regulated operations of the kiosk.

2.5.2 Printed Circuit Board (PCB) Identification Requirements

Each PCB must be clearly identifiable by an alphanumeric identification and, when applicable, a revision number. If track cuts, patch wires, or other circuit alterations are introduced to the PCB, then a new revision number must be assigned.

2.5.3 Switches and Jumpers

If the kiosk contains switches and/or jumpers, they must be fully documented for evaluation by the independent test laboratory.

2.5.4 Kiosk Wiring

The kiosk terminal must be designed so that power and data cables into and out of the kiosk terminal can be routed so that they are not accessible to the public.

NOTE: The independent test laboratory will make no determination as to whether the kiosk installation conforms to local electrical codes, or to any other electrical testing standards and practices.

2.5.5 Wired Communication Ports

Wired communication ports must be clearly labeled and must be securely housed within the kiosk terminal to prevent unauthorized access to the ports or their associated cable connectors.

2.5.6 Charging Mechanisms

The kiosk may support the use of an externally accessible charging mechanism, such as a Universal Serial Bus (USB) charging port, or some other analogous technology (e.g., cables, inductive chargers, etc.). The mechanism may be used to provide external power or charging access for an electronic device such as a smartphone, tablet, etc. If so equipped, the charging mechanism shall:

a) Be appropriately fused and/or electrically-protected; and
b) Not impact the integrity of the regulated operations of the kiosk.

2.6 Doors and Security

2.6.1 General Statement

This section is only applicable for a kiosk terminal which:

a) Performs transactions using peripheral devices installed within the terminal; and/or
b) Has locally stored critical NV memory and/or installed software which has the potential to influence the regulated operations of the kiosk.

2.6.2 Physical Security

The kiosk terminal must be robust enough to resist forced entry into any secured doors, areas, or compartments. In the event that extreme force is applied to the cabinet materials causing a potential

breach in kiosk terminal security, evidence of tampering must be conspicuous. "Secured areas" or "secured compartments" must include, as applicable, the external doors such as the main door, currency compartment doors such as a drop box door or stacker door, and/or other sensitive access areas of the kiosk terminal.

2.6.3 External Doors

The following requirements apply to kiosk terminals which contain external doors into any secured areas or compartments:

a) External doors must be manufactured of materials that are suitable for allowing only legitimate access to the inside of the kiosk terminal.
b) External doors and their associated hinges must be capable of withstanding determined and unauthorized efforts to gain access to the interior of the kiosk terminal and must leave conspicuous evidence of tampering if such an attempt is made;
c) The seal between the kiosk terminal and the external door must be designed to resist the entry of objects. It must not be possible to insert an object into the kiosk terminal that disables a door open sensor when the kiosk terminal's door is fully closed, without leaving conspicuous evidence of tampering; and
d) All external doors must be secure and support the installation of locks.

2.6.4 Door Monitoring

Any doors that provide access to secure areas of the kiosk terminal must be monitored by door access detection software.

a) The detection software must register a door as being open when the door is moved from its fully closed and locked position, provided power is supplied to the kiosk.
b) When any door that provides access to a secured area or secured compartment registers as open, the kiosk must cease operation and display an appropriate error message. This error condition shall be communicated to the back-office platform when such functionality is supported.

2.7 Peripherals

2.7.1 Peripheral Requirements

A peripheral is defined as an internal or external device connected to the kiosk terminal that supports credit acceptance, credit issuance, player identification, or other specialized function(s) which are used in the regulated operations of the kiosk. The following requirements apply for kiosk peripherals as supported:

a) Bill validators and stackers must meet the applicable jurisdictional requirements for bill validators. In the absence of specific jurisdictional standards, the requirements established within the "Bill Validators and Stackers" section of the *GLI-11 Standards for Gaming Devices* must be used as applicable.

b) Coin acceptors, diverters, and drop boxes must meet the applicable jurisdictional requirements for coin acceptors. In the absence of specific jurisdictional standards, the requirements established within the "Coin Acceptors, Diverters, and Drop Boxes" section of the *GLI-11 Standards for Gaming Devices* must be used as applicable.
c) Integrated player identification components must meet the applicable jurisdictional requirements for these components. In the absence of specific jurisdictional standards, the requirements established within the "Integrated Player Identification Components" section of the *GLI-11 Standards for Gaming Devices* must be used as applicable. This does not apply to the use of kiosks for player tracking only or for the redemption of promotional player points for merchandise and/or services.
d) Hoppers and/or printers must meet the applicable jurisdictional requirements for these devices. In the absence of specific jurisdictional standards, the requirements established within the "Machine Payment and Payment Devices" and "Machine Vouchers" sections of the *GLI-11 Standards for Gaming Devices* must be used as applicable.

NOTE: The requirement for error conditions within the above referenced sections to "sound an alarm and/or illuminate the tower light" is not applicable for kiosks. However, these error conditions must be communicated to the back-office platform when such functionality is supported. Additionally, the "Bill Validator Recall" and "Voucher-Out Log" are not required if the "Transaction Log" specified in the next chapter contains these transactions.

Chapter 3: Kiosk Software Requirements

3.1 Introduction

3.1.1 General Statement

This chapter sets forth the requirements for the kiosk software. Kiosk software refers to the software used to take part in regulated operations which, based on design, is downloaded to or installed on the kiosk terminal, run from the back-office platform, or a combination of the two.

3.2 Software Requirements

3.2.1 Software Identification

Kiosk software must contain sufficient information to identify the software revision level.

3.2.2 Software Validation

The kiosk and/or back-office platform must have the ability to authenticate that all regulated critical components contained in any kiosk software are valid each time the software is loaded for use and, where supported by the system, on demand. Critical components may include but are not limited to elements that control kiosk communications, peripheral device firmware, or other components that affect regulated operations of the kiosk.

a) The authentication must employ a hash algorithm which produces a message digest of at least 128 bits. Other test methodologies shall be reviewed on a case-by-case basis.
b) In the event of a failed authentication (i.e., program mismatch or authentication failure), the kiosk must cease operation and display an appropriate error message. This error condition must be communicated to the back-office platform when such functionality is supported.

NOTE: Program verification mechanisms will be evaluated on a case-by-case basis and approved by the regulatory body and the independent test laboratory based on industry-standard security practices.

3.2.3 Independent Software Verification

It must be possible to perform an independent integrity check of the kiosk software from an outside source. This verification is required for all control programs that affect the integrity of the kiosk. The verification must be accomplished by being authenticated by a third-party application run from the kiosk and/or back-office platform, by allowing a third-party device to authenticate the media, or by allowing for removal of the media such that it can be verified externally. The independent test laboratory, prior to software approval, must evaluate the integrity check method.

3.3 Critical Non-Volatile (NV) Memory

3.3.1 Contents of Critical NV Memory

Critical Non-Volatile (NV) memory must be used to store all data elements that are considered vital to the continued operation of the kiosk software. Critical NV memory may be maintained by the kiosk and/or the back-office platform. These data elements include, but are not limited to:

a) All electronic meters and logs defined in the "Electronic Meters and Logs" section of this standard;
b) Current kiosk balance (as applicable); and
c) Kiosk configuration data (e.g., communications, etc.) and state of operations (e.g., error conditions, etc.).

3.3.2 Critical NV Memory Backup

Kiosks whose operation relies on locally stored critical NV memory must have a backup or archive capability, which allows the recovery of critical NV memory should a failure occur.

3.3.3 Critical NV Memory Errors

Critical NV memory storage must be maintained by a methodology that enables errors to be identified. This methodology may involve signatures, checksums, redundant copies, database error checks, and/or other method(s) approved by the regulatory body.

3.3.4 Critical NV Memory Checks

Comprehensive checks of critical NV memory data elements must be made upon power up and program resumption. NV memory that is not critical to kiosk integrity is not required to be checked.

3.3.5 Unrecoverable Corruption of Critical NV Memory

An unrecoverable corruption of critical NV memory, must result in an error. Upon detection, the kiosk software must cease operation and display an appropriate error message. Additionally, the critical NV memory error must cause any communication external to the kiosk to cease.

NOTE: This 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.

3.4 Kiosk Operations

3.4.1 Player Interface Requirements

The player interface is defined as an application or program through which the player views and/or interacts with the kiosk software. The player interface must meet the following:

a) The functions of all buttons, touch or click points must be clearly indicated within the area of the button, or touch/click point and/or within the help menu. There must be no functionality available through any buttons or touch/click points on the player interface that are hidden or undocumented.
b) Any resizing or overlay of the player interface must be mapped accurately to reflect the revised display and touch/click points.
c) Player interface instructions, as well as information on the functions and services provided by the kiosk, must be clearly communicated to the player and must not be misleading or inaccurate.
d) The display of this information must be adapted to the player interface. For example, where a kiosk uses technologies with a smaller display screen, it is permissible to present an abridged version of this information accessible directly from within the transaction screen and make available the full/complete version of this information via another method, such as a secondary screen, help menu, or other interface that is easily identified on the visual transaction screen.

3.4.2 Simultaneous Inputs

The kiosk software must not be adversely affected by the simultaneous or sequential activation of the various inputs and outputs which might, whether intentionally or not, cause malfunctions or invalid results.

3.4.3 Current Kiosk Balance

Where applicable, the current kiosk balance must be displayed to the player any time a transaction may be conducted unless a tilt condition or malfunction exists, or unless the player opts to view an informational screen such as a menu or help screen item. The amount displayed must be updated upon every transaction performed.

3.5 Kiosk Configurations and Functionality

3.5.1 Configuration Settings

Changes to any configuration settings for the regulated operations of the kiosk may only be performed by a secure means.

3.5.2 Transaction Limits

The kiosk software must have the ability to configure transaction limits, where required by the regulatory body. If a player attempts a transaction which exceeds these limits, then this transaction may only be processed provided that the player is clearly notified that they have transacted less than requested.

3.5.3 Bill Breaking/Dispensing Functionality

If allowed by the regulatory body, the kiosk software may have the functionality of acting as a bill breaker/dispenser. The bill dispenser software for bill-breaking must have preset amounts, player

selection or the option to set dispensing amounts. The kiosk must identify options on bill dispensing selectable options on denominations when bill dispensing.

3.5.4 Automated Teller Machine (ATM) Functionality

If allowed by the regulatory body, the kiosk software may have the ability to issue funds from an automated teller machine (ATM) network however, the ATM network must not interact with the host system and the kiosk must be capable of separately identifying and summarizing ATM transactions from other transactions.

NOTE: The independent test laboratory does not make any findings with regard to evaluating or certifying ATM functionality as such requirements fall under Federal (Banking) Regulations. It is the responsibility of the manufacturer of the kiosk and provider of ATM services to ensure these regulations are met prior to installation.

3.6 Communication Protocol

3.6.1 Integrity of Protocol Communications

The kiosk software must accurately function as indicated by the communications protocol that is implemented, and as required by the regulatory body. In addition, the following rules must be met:

a) The kiosk software must be designed or programmed such that it may only communicate with authorized system components through secure communications.
b) After a program interruption, any communications to an external device must not begin until the program resumption routine, including any self-test, is completed successfully.
c) If communication between the kiosk and the host system is lost, the kiosk software must cease operations related to that communication and display an appropriate error message. It is permissible for the kiosk software to detect this error when the kiosk tries to communicate with the system. Non-system transactions, such as bill breaking if supported, may continue while system communication is down.

3.6.2 Protection of Sensitive Information

The kiosk software must not allow any information contained in communication to or from the kiosk that is intended by the communication protocol to be protected, or which is of a sensitive nature, to be viewable through any display mechanism supported by the kiosk. This includes, but is not limited to, secure PINs, player data, or secure seeds and keys.

3.6.3 Kiosk Communication

Any kiosk which is capable of bidirectional communication with internal or external associated equipment, or other equipment, must utilize a robust communication protocol which ensures that erroneous data or signals do not adversely affect the integrity or operation of the kiosk.

3.6.4 Kiosk Clock

If the kiosk maintains an internal clock, it must be able to accurately reflect the current time and date and synchronize its clock to that of the host system.

3.7 Electronic Meters and Logs

3.7.1 Information Access

The electronic meters and logs must only be accessible by an authorized person and must have the ability to be displayed on demand using a secure means.

3.7.2 Electronic Accounting Meters

Electronic accounting meters must be at least ten (10) digits in length. Eight (8) digits must be used for the dollar amount and two (2) digits used for the cents amount. The meter must automatically roll over to zero once its maximum logical value has been reached. Meters must be labeled so they can be clearly understood in accordance with their function. The required electronic accounting meters are as follows:

a) Handpay. The kiosk software must have a meter that accumulates the total value of payments made by an attendant when the kiosk is incapable of making the proper payment;
b) Physical Coin In. The kiosk software must have a meter that accumulates the total value of coins or tokens inserted into the kiosk;
c) Physical Coin Out. The kiosk software must have a meter that accumulates the total value of coins or tokens physically paid by the kiosk;
d) Bill In. The kiosk software must have a meter that accumulates the total value of currency accepted;
e) Bill Out. The kiosk software must have a meter that accumulates the total value of currency physically paid by the kiosk;
f) Voucher In. The kiosk software must have a meter that accumulates the total value of all wagering vouchers accepted by the kiosk;
g) Voucher Out. The kiosk software must have a meter that accumulates the total value of all wagering vouchers issued by the kiosk;
h) Electronic Funds Transfer In (EFT In). The kiosk software must have a meter that accumulates the total value of cashable credits electronically transferred to the kiosk from a financial institution through a host system;
i) Player Account Transfer In (WAT In). The kiosk software must have a meter that accumulates the total value of cashable credits electronically transferred to the kiosk from a player account through a host system;
j) Player Account Transfer Out (WAT Out). The kiosk software must have a meter that accumulates the total value of cashable credits electronically transferred from the kiosk to a player account through a host system;
k) Cashable Electronic Promotion In (CEP In). The kiosk software must have a meter that accumulates the total value of cashable credits electronically transferred to the kiosk from a player account through a host system;

l) Cashable Electronic Promotion Out (CEP Out). The kiosk software must have a meter that accumulates the total value of cashable credits electronically transferred from the kiosk to a player account through a host system;
m) Non-Cashable Electronic Promotion In (NCEP In). The kiosk software must have a meter that accumulates the total value of non-cashable credits electronically transferred to the kiosk from a player account through a host system;
n) Non-Cashable Electronic Promotion Out (NCEP Out). The kiosk software must have a meter that accumulates the total value of non-cashable credits electronically transferred from the kiosk to a player account through a host system;
o) Coupon Promotion In. The kiosk software must have a meter that accumulates the total value of all promotional coupons accepted by the kiosk;
p) Coupon Promotion Out. The kiosk software must have a meter that accumulates the total value of all promotional coupons issued by the kiosk; and
q) Other Meters. Kiosk software that allows for transactions related to regulated operations of the kiosk that would not otherwise be metered under any of the above electronic accounting meters, must maintain sufficient meters to properly reconcile all such transactions.

NOTE: Any accounting meter that is not supported by the functionality of the kiosk, is not required to be implemented by the supplier.

3.7.3 Electronic Occurrence Meters

Occurrence meters must be at least eight (8) digits in length however, are not required to automatically roll over. Meters must be labeled so they can be clearly understood in accordance with their function. The required electronic occurrence meters are as follows:

a) External Doors. The kiosk software must have meters that accumulate the number of times any external door (e.g., main or belly door, drop box door, currency area with an external door, etc.) has been opened since the last NV memory clear, provided power is supplied to the kiosk.
b) Stacker Door. The kiosk software 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 kiosk;
c) Bill Denomination In. The kiosk software must have a specific occurrence meter for each denomination of currency accepted by the kiosk;
d) Bill Denomination Out. The kiosk software must have a specific occurrence meter for each denomination of currency dispensed by the kiosk;
e) Wagering Instruments Accepted. The kiosk software must have a specific occurrence meter that records the number of all other notes not including bills, such as vouchers and coupons, accepted by the kiosk; and
f) Wagering Instruments Issued. The kiosk software must have a specific occurrence meter that records the number of all other notes not including bills, such as vouchers and coupons, issued by the kiosk.

NOTE: Any occurrence meter that is not supported by the functionality of the kiosk, is not required to be implemented by the supplier.

3.7.4 Transaction Log

There must be the capacity to display a complete transaction log for the previous thirty-five (35) transactions that incremented any of the meters related to bills, wagering instruments, EFT, and player account transactions. The following information must be displayed:

a) The transaction value in local monetary units in numerical form;
b) The time of day of the transaction, in twenty-four (24) hour format showing hours and minutes;
c) The date of the transaction, in any recognized format, indicating the day, month, and year;
d) For wagering instrument transactions, the validation number with the following conditions:
    i. Where the log can be displayed by the kiosk terminal, only the last four (4) digits may be displayed for voucher-out transactions where the vouchers haven't been redeemed yet;
    ii. Where the log can be displayed from back-office platform, at least the last four (4) digits must be displayed for voucher-in transactions;
e) For player account transactions:
    i. The type of transaction (upload/download) including restrictions (cashable or non-cashable, etc.); and
    ii. The account number or a unique transaction number, either of which can be used to authenticate the source of the funds (i.e. where funds came from/went to).

NOTE: It is acceptable for items accepted by the bill validator to be omitted from this log if there is a timestamped bill validator recall log maintained which indicates the item type and denomination/value for last five (5) items accepted by the bill validator. It is also acceptable for issued vouchers to be omitted from this log if there is a timestamped voucher-out log maintained which indicates the above information for the last twenty-five (25) issued vouchers.

3.7.5 Significant Event Log

The last one hundred (100) significant events for kiosks must be stored with an appropriate timestamp in one or more secure logs that are not accessible to the player and which minimally include the following events, as applicable:

a) Software verification errors or critical NV memory errors, if technically possible to log these events based on the nature and/or severity of the error;
b) Changes made to kiosk configurations;
c) Kiosk communication failure, if supported;
d) Power resets;
e) Handpay conditions;
f) Access to secured areas or secured compartments; and
g) Peripheral errors, if supported.

Glossary of Key Terms

Back-office Platform – A kiosk component external to the kiosk terminal which may govern some or all the regulated operations of the kiosk, such as metering and communications between the host system and the kiosk terminal. The back-office platform may be integrated into the host system. For the purposes of this technical standard, the back-office platform is considered a part of the kiosk.

Barcode – An optical machine-readable representation of data. A good example is a barcode found on printed vouchers.

Barcode Reader – A device that is capable of reading or interpreting a barcode. This may extend to some smartphones or other electronic devices that can execute an application to read a barcode.

Bill In/Out – The total value of all currency accepted or paid out by a bill validator.

Bill Validator – A kiosk peripheral that accepts paper currency, wagering instruments, and other approved items in exchange for credits.

Card Reader – A kiosk peripheral that reads data embedded on a magnetic strip, or stored in an integrated circuit chip, for player identification.

Cashable Credits (aka "Unrestricted Credits") – Credits that are redeemable for cash.

CEP, *Cashable Electronic Promotion* – Cashable credits electronically transferred to/from a kiosk from/to a promotional account.

Coin Acceptor – A kiosk peripheral that accepts coins or tokens in exchange for credits. The coin-in assembly receives, verifies, counts and appropriately routes coins deposited into the machine.

Control Program – A software program that controls kiosk behaviors relative to any applicable technical standard and/or regulatory requirement.

Coupon – A wagering instrument that is used primarily for promotional purposes and which can be redeemed for cashable or non-cashable credits.

Coupon Promotion In/Out – The total value of all promotional coupons accepted or paid out by the kiosk.

Critical Non-Volatile (NV) Memory – Memory used to store all data that is considered vital to the continued operation of the kiosk.

Diverter – The portion of the coin-in assembly that channels coins to either the hopper or the drop box.

Drop Box – A secure container housed within a kiosk cabinet that collects coins when the hopper is full or when the diverter directs coins to it.

EFT, *Electronic Funds Transfer; ECT, Electronic Credits Transfer* – EFT (or ECT) is a system by which currency can be electronically transferred to or from a kiosk in the form of credits. EFT requires some form of communication between the kiosk and a host system.

Electronic Accounting Meter (aka "Software Meter" / "Soft Meter") – An accounting meter that is implemented in the main program software of a kiosk.

EMC, *Electromagnetic Compatibility* – The principal in which any electronic or electrical appliance should be able to operate without causing, or being affected by, electromagnetic interference.

EMI, *Electromagnetic Interference* – Any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment.

ESD, *Electro-Static Discharge* – The release of static electricity when two objects come into contact. It is the sudden flow of electricity between two electrically charged objects caused by contact, an electrical short, or a dielectric breakdown.

Hopper – An electromechanical assembly inside the kiosk that receives, holds and dispenses coins and/or currency.

Integrated Player Identification Component – An integrated player identification component is an electronic device controlled by kiosk software which provides a means for players to enter their secure identification information. Examples include a card reader, a barcode reader, or a biometric scanner.

Jumper – A removable connector (plug, wire, etc.) that electrically joins together or short-circuits two separate physical connections.

Kiosk – Kiosks are player interface units that may be used to perform regulated operations when interfaced with a compatible host system. This includes the kiosk terminal and the back-office platform.

Kiosk Software – The software used to take part in regulated operations which, based on design, is downloaded to or installed on the kiosk terminal, run from the back-office platform, or a combination of the two.

Kiosk Terminal – An electronic device that converts communications from the kiosk software into a human interpretable form and converts human decisions into communication format understood by the kiosk software.

MI, *Magnetic Interference* – Any magnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment.

NCEP, *Non-Cashable Electronic Promotion* – Non-cashable credits electronically transferred to/from the kiosk from a promotional account.

Non-Cashable Credits (aka "Restricted Credits") – Credits that have no cash redemption value.

PCB, *Printed Circuit Board* – A hardware component of a computer or other electronic device, consisting of a flat piece of a non-conductive, rigid material to which Integrated Circuits (ICs) and other electronic components such as capacitors, resistors, etc. are mounted. Electrical connections are made between the ICs and components using a copper sheet that is laminated into the overall board assembly.

Peripheral – An internal or external device connected to a machine that supports credit acceptance, credit issuance, player interaction, or other specialized function(s).

Physical Coin In/Out – The total value of coins or tokens inserted into or paid out by the kiosk.

PIN, *Personal Identification Number* – A numerical code associated with an individual and which allows secure access to a domain, account, network, system, etc.

Player Account (aka "Wagering Account" / "Cashless Account") **–** An account maintained for a player where information relative to financial and wagering/gaming transactions are recorded on behalf of the player including, but not limited to, deposits, withdrawals, wagers, winnings, and balance adjustments. The term does not include an account used solely by an operator to track promotional points or credits or similar benefits issued by an operator to a player which may be redeemed for merchandise and/or services.

Player Account Transfer (aka "Wagering Account Transfer" / "Cashless Account Transfer") – Cashable credits electronically transferred to/from the kiosk from a player account.

Player Data – Sensitive information regarding a player and which may include items such as full name, date of birth, place of birth, social security number, address, phone number, medical or employment history, or other personal information as defined by the regulatory body.

Printer – A kiosk peripheral that prints wagering instruments and other items as necessary.

Protocol – A set of rules and conventions that specifies information exchange between devices, through a network or other media.

RFI, *Radio Frequency Interference* – Electromagnetic radiation which is emitted by electrical circuits carrying rapidly changing signals, as a by-product of their normal operation, and which causes unwanted signals (interference or noise) to be induced in other circuits.

Secure Areas or Secure Compartments – Sensitive areas of a kiosk such as the external doors such as the main door, currency compartment doors such as a drop box door or stacker door, and/or other sensitive access areas of the kiosk terminal.

Sensitive Information – Includes information such as PINs, player data, passwords, secure seeds and keys, and other data that must be handled in a secure manner.

Stacker – An electromechanical bill validator component that loads paper currency, wagering instruments, and other approved items into a locked container for secure storage within the kiosk.

Tilt – An error in kiosk operation that halts or suspends operations and/or that generates some intelligent fault message.

Touch Screen – A video display device that also acts as a player input device by using electrical touch point locations on the display screen.

Voucher – A wagering instrument which can be redeemed for cash or used to subsequently redeem for credits.

Voucher In/Out (aka "Ticket In/Out") – The total value of all wagering vouchers accepted or paid out by the kiosk.

Wagering Instrument – A printed or virtual representative of value, other than a chip or token and includes coupons and vouchers. A virtual wagering instrument is an electronic token exchanged between a player's mobile device and the kiosk which is used for credit insertion and redemption.