

# TECHNICAL STANDARDS FOR GAMING DEVICES AND ASSOCIATED EQUIPMENT

(Draft Date January 11, 2016)

New

~~[Deleted]~~

## STANDARD 1

### INTEGRITY OF GAMING DEVICES

#### 1.020 Electrical interference immunity.

1. A conventional gaming device or client must exhibit total immunity to human body electrostatic discharges on all player-exposed areas. For purposes of this standard, a human body discharge is considered to be an electrical potential of not greater than 20,000 volts DC discharged through a network with a series resistance of 150 to 1500 ohms shunted by a capacitance of 100 to 150 picofarads. The device must withstand this discharge repeated at one-second intervals. The power source for this human body equivalent is a high-impedance source such that, in effect, the energy available for a given discharge is limited to that contained in the shunt capacitor.

2. A gaming device may exhibit temporary disruption when subjected to electrostatic discharges of 20,000 to 27,000 volts DC through a network with a series resistance of 150 to 1500 ohms shunted by a capacitance of 100 to 150 picofarads, but must exhibit a capacity to recover and complete an interrupted play without loss or corruption of any stored or displayed information and without component failure.

3. Gaming device power supply filtering must be sufficient to prevent disruption of the device by repeated switching on and off of the AC power. The device must not exhibit disruption when a 1 microfarad capacitor, charged to plus or minus 680 volts DC is discharged between the hot and neutral AC supply lines, at any phase from zero to 360 degrees, with a repetition rate of 30 times per second.

~~[4.—The random number generator and random selection process must be impervious to influences from outside the device, including, but not limited to, electro-magnetic interference, electro-static interference, and radio frequency interference. A gaming device must use appropriate communication protocols to protect the random number generator and random selection process from influence by associated equipment which is conducting data communications with the gaming device.]~~

4. This section does not apply to devices provided by a patron used to conduct gaming activity or interact with a gaming device. Such devices include, but are not limited to smartphones and tablets.

5. A manufacturer may request a waiver from the chairman of this section for gaming devices that are certified by an OSHA Nationally Recognized Testing Laboratory for electrical interference immunity.

(Adopted: 9/89. Amended: 11/05; 11/17/05)

#### 1.030 Coin acceptor and receiver.

1. Coin (or token) acceptors must be designed to accept designated coins or tokens and reject others. The coin receiver on a gaming device must be designed in a manner that minimizes the potential for use of cheating methods such as slugging, stringing or spooning.

2. Gaming devices which are configured to accept more than 20 coins or tokens for a single play must use a coin acceptor that accepts or rejects on the basis of metal composition of the coin or token unless the denomination of the coin or token is \$.05 or less.

(Adopted: 9/89. Amended: 11/20/97; 7/26/07)

#### 1.035 Change vouchers or coupons.

1. A wagering instrument inserted into a gaming device that is less in amount than that gaming device's smallest denomination shall:

(a) Cause that gaming device to immediately reject the wagering instrument if that gaming device does not have an odd cents meter; or

(b) Allow for the additional accumulation of wagering credits if the gaming device has an odd cents meter.

2. A wagering instrument inserted into a gaming device that is greater in amount than that gaming device's smallest denomination and not evenly divisible by any of the gaming device's denominations shall:

(a) Cause that gaming device to immediately issue a change voucher or coupon if that gaming device does not have an odd cents meter and is equipped with a printer mechanism;

(b) Allow for the additional accumulation of wagering credits; or

(c) Cause that gaming device to immediately reject the wagering instrument if that gaming device is not equipped with a printer mechanism or if the printer mechanism is not functioning for any reason.

(Adopted: 5/03. Effective: 2/1/04)

**1.040 Hoppers.** The hopper mechanism on gaming devices must be designed to detect jammed coins, extra coins paid out, hopper runaways, and hopper empty conditions. The device control program must monitor the hopper mechanism for these error conditions in all active game states that do not indicate error conditions.

(Adopted: 9/89)

#### **1.045 Printers.**

1. Printer mechanisms on gaming devices must be designed to allow the gaming device to detect low paper, paper out, ~~presentation error~~, printer failure, and paper jam conditions.

2. Printers must be mounted inside a lockable area of the gaming device.

(Adopted: 5/03. Amended: 1/1/05. Section (1) effective 2/1/04. Section (2) effective 1/1/05)

#### **1.050 Physical security.**

1. A conventional gaming device must resist forced illegal entry and must retain evidence of any entry until properly cleared or until a new play is initiated. A gaming device must have a protective cover over the circuit boards that contain programs and circuitry used in the random selection process and control of the gaming device, including any electrically alterable program storage media. The cover must be designed to permit installation of a security locking mechanism by the manufacturer or end user of the gaming device.

2. A system supported game must:

(a) For the client portion of the system supported game, comply with Technical Standard 1.050(1).

(b) For the system portion of the system supported game, the server or system component must reside in a secure area where access is limited to authorized personnel. Gaming device application access to the system supported game shall be logged on the server or system component and remotely on a secondary logging device which resides outside the secure area and is not accessible to the individual accessing the secure area. A system supported game is not required to log this information on the secondary logging device if the information has been rendered unalterable, through a means approved by the Chairman, on the server or system part of the gaming device. Logged data shall include: time and date of the access and the identification of the accessing individual(s). The resulting logs shall be retained for a minimum of 90 days.

3. A system based game must:

(a) For the client portion of the system based game, comply with Technical Standard 1.050(1).

(b) For the system portion of the system based game, the server or system component must reside in a secure area where access is limited to authorized personnel. Gaming device application access to the system based game must be logged automatically on the system component of the game and on a computer or other logging device that resides outside the secure area and is not accessible to the individual(s) accessing the secure area. A system based game is not required to log this information on the secondary logging device if the information has been rendered unalterable, through a means approved by the Chairman, on the server or system part of the gaming device. The logged data shall include the time, date, and the identity of the individual accessing the secure area. The resulting logs must be kept for a minimum of 90 days. Additionally, a dedicated video camera specifically installed to monitor access to the system based game must record all accesses to the secure area and the resulting video log must be retained for a period of at least 7 days.

(Adopted: 9/89. Amended: 11/20/97; 11/17/05; 8/8/11)

**1.060** ~~[Communication with associated equipment.]~~ Gaming Device Communications

1. Any gaming device which is capable of bidirectional communication with internal or external associated equipment or other equipment must utilize a communication protocol which insures that erroneous data or signals will not adversely affect the operation of the device.

2. Any new or modified gaming device submitted for approval which is used with a progressive controller or any other associated equipment that is intended to signal a jackpot hit of any level must provide a complex signal consisting of at least eight logical transitions involving time and magnitude. The device may optionally provide an additional jackpot signal intended for use with older progressive equipment.

3. System supported and system based games may only communicate with equipment or programs external to the system supported or system based game through a secure interface. This interface will specifically not allow any external connection to directly access the internal components, software or data of the system supported or system based gaming device. The interface must:

(a) Be based on a specific defined protocol or a specific set of defined commands and as a result of these commands, retrieve information for an external request;

(b) Place data in an area sufficiently segregated from the system supported or based game software that is available to external requests or associated equipment; or

(c) Be of a suitable design capable of supplying requested information while isolating the external request or equipment from the system supported or system based game internal components, software or data.

4. Software transferred between server and client or conventional gaming device portions of a system based or system supported game must be conducted using a method that securely links the client or clients to the server such that the software may only be used by authorized clients. In general, if certificates, keys or seeds are used they must not be hard coded, and must change automatically, over time, as a function of the communication.

5. Information related to player input, game outcome, financial transactions, and game recall information must be encrypted by a means approved by the Chairman.

6. Internet accessibility

(a) A gaming device, other than an interactive gaming device, may not directly access or be directly accessed via the internet.

(b) A gaming device, other than an interactive gaming device, may indirectly access the internet or be accessed indirectly via the internet using a method that securely isolates and segregates the gaming device from the internet.

7. Communication between a gaming device and any device external or internal to the gaming device conducted using wireless transmission technologies such as Near Field Communications, Bluetooth, or WiFi must:

(a) Be secured to prevent the ability of unintended recipients to read the data;

(b) Employ a method to detect data corruption. Upon detection of corrupt data, correct or terminate the communication; and

(c) Employ a method to prevent modification of the data.

(Adopted: 9/89. Amended: 11/17/05)

~~**1.062 Communication between Client or Conventional Gaming Device and Servers or System Portions of a Gaming Device.**~~

~~1.—Software transferred between server and client or conventional gaming device portions of a system based or system supported game must be conducted using a method that securely links the client or clients to the server such that the software may only be used by authorized clients. In general, if certificates, keys or seeds are used they must not be hard coded, and must change automatically, over time, as a function of the communication.~~

~~2.—Information related to player input, game outcome, financial transactions, and game recall information must be encrypted by a means approved by the Chairman.]~~

(Adopted: 11/17/05)

~~**1.066 Remote access to gaming devices. Remote access includes all access to a gaming device from outside the gaming device or gaming device network including access from other networks within the same establishment.**~~

~~Remote access includes all access to a gaming device from outside the gaming device or gaming device network including access from other networks within the same establishment.~~

1. Remote access to a gaming device may only be conducted with the server or system portion of a system supported or system based game.

2. Remote access to a gaming device may only be granted for the following activities:

- (a) Monitoring system health and performance;
- (b) Scheduling operational gaming device functions such as downloading of content;
- (c) Troubleshooting system issues;
- (d) Performing inquiry-only functions such as viewing logs or generating reports
- (e) Any other activity that is approved by the Chairman.

3. A gaming device must be securely isolated from any remote access connection through a means approved by the Chairman.

4. A gaming device may only be accessed using a method that securely links the gaming device to the remote system requesting access. This secure link must uniquely identify the remote system requesting access as an entity authorized to conduct remote communications with the gaming device.

5. A gaming device must provide a hardware or software mechanism that will sever the connection between the gaming device and the remote access terminal unless persistent remote access is implemented for the purpose of monitoring system health and performance. This device must default to and must remain in the disconnected state unless specifically set to allow communications as a result of a command issued by the gaming device. Additionally, upon completion of the communications, the device must again sever the connection between the gaming device and the remote access terminal.

6. A gaming device must log each remote access on the server or system part of the gaming device and on the secondary logging device. A system supported game is not required to log this information on the secondary logging device if the information has been rendered unalterable, through a means approved by the Chairman, on the server or system part of the gaming device. The log must include time and date of the access and a list of programs transferred or changed.

7. A system based game must not enable remote access unless the secondary logging device, if used to comply with these standards, is operational and is communicating with the gaming device.

8. If a gaming device allows for downloading of new gaming device applications or gaming device related firmware through remote access, the software downloaded to a system based or system supported game must be initially stored in a separate area or partition of memory such that the software is sufficiently segregated from the system based or system supported gaming device's operating software as to be unable to affect the operation of the gaming device.

9. If a gaming device allows for downloading of new gaming device applications or gaming device related firmware through remote access, the software downloaded to a system supported or system based game must be completely authenticated prior to performing any operation on the software including, but not limited to, decrypting, extracting, uncompressing or installation.

Note: For the purposes of these regulations "gaming device network" means any method used and the components employed by a licensee to facilitate the operations of a system based or system supported gaming device.

(Adopted: 11/17/05; 8/8/11)

### **1.070 Error conditions.**

1. Gaming devices must detect and display the following conditions during idle states or game play. These conditions may be automatically cleared by the gaming device upon completion of a new play sequence or the initiation of a new play sequence if the gaming device maintains a log of the most recent error condition and the previous thirty-four error conditions.

- (a) Power reset.
- (b) Door open.
- (c) Door just closed.
- (d) Inappropriate coin-in if the inappropriate coin(s) in are not returned to the player.

2. Gaming devices must be capable of detecting and displaying the following error conditions which must disable game play and may only be cleared by an attendant:

- (a) Coin-in error (coin jam, reverse coin-in, etc.).
- (b) Coin-out error (coin jam, extra coin paid out, etc.).
- (c) Hopper empty or timed-out (Hopper failed to make payment).
- (d) Hopper runaway.
- (e) Low RAM battery (a designated battery replacement schedule may be used in lieu of a low battery detection scheme).
- (f) Print failure, if the gaming device has no other means to make a payout. A replacement voucher may be printed once the failure condition has been cleared.
- (g) Printer mechanism paper jam. A paper jam condition must be monitored at all times during the print process.
- (h) Printer mechanism paper out, if the gaming device has no other means to make a payout.
- (i) Program error (Defective program storage media).
- (j) Reel spin error of any type including a mis-index condition for mechanical reels. The specific reel number must be identified. If a tilt occurs while the reel(s) are spinning the gaming device must spin the reel(s) at a slow speed.
- (k) Removal of control program storage media.
- (l) Uncorrectable RAM error (RAM defective or corrupted).

3. Gaming devices must be capable of detecting and displaying the following error conditions which must be cleared by an attendant. Game play may continue if an alternative method is available to complete the transaction or the condition does not prohibit the transaction from being completed.

- (a) Hopper empty or timed-out (Hopper failed to make payment).
- (b) Printer mechanism low paper.

~~[(e)]~~ ~~[Presentation error.]~~

~~[(d)]~~(c) Print failure.

~~[(e)]~~(d) Printer mechanism paper out.

4. A description of device error codes and their meanings must be affixed inside the gaming device unless the displayed device error codes are self-explanatory.

(Adopted: 9/89. Amended: 5/03; 1/1/05; 8/8/11)

### 1.080 Control program requirements.

1. All gaming devices which have control programs residing in one or more Conventional ROM Devices must employ a mechanism approved by the chairman to verify control programs and data. The mechanism used must detect at least 99.99 percent of all possible media failures. If these programs and data are to operate out of volatile RAM, the program that loads the RAM must reside on and operate from a Conventional ROM Device.

2. All gaming devices having control programs or data stored on memory devices other than Conventional ROM Devices must:

(a) Employ a mechanism approved by the chairman which verifies that all control program components, including data and graphic information, are authentic copies of the approved components. The authentication mechanism must employ a hashing algorithm which produces a message digest output of a least 128 bits. If the message digest is stored on a memory device other than a Conventional ROM Device the digest must be encrypted using a public/private key algorithm with a minimum of a 512 bit key. The mechanism must prevent the execution of any control program component if any component is determined to be invalid. Any program component of the verification initialization mechanism must be stored on a Conventional ROM Device that must be capable of being authenticated using a method approved by the chairman.

(b) Employ a mechanism approved by the chairman which tests unused or unallocated areas of any alterable media for unintended programs or data and tests the structure of the storage media for integrity. The mechanism must prevent further play of the gaming device if unexpected data or structural inconsistencies are found.

(c) Provide a mechanism for keeping a record, in a form approved by the chairman, anytime a control program component is added, removed, or altered on any alterable media. The record must contain a minimum of the last 10 modifications to the media and each record must contain the date and time of the action, identification of the component affected, the reason for the modification and any pertinent authentication information.

(d) Provide, as a minimum, a two-stage mechanism for verifying all program components on demand via a communication port and protocol approved by the chairman. The mechanism must employ a hashing algorithm which produces a messages digest output of a least 128 bits and must be designed to accept a user selected authentication key or seed to be used as part of the mechanism (i.e. HMAC SHA-1). The first stage of this mechanism must allow for verification of all control components. The second stage must allow for the verification of all program components, including graphics and data components in a maximum of 20 minutes. The mechanism for extracting the verification information must be stored on a Conventional ROM Device. **[Effective 11/1/2012]** All gaming devices must also provide the same two-stage mechanism for verifying all program components on demand via a gaming device user interface where the results are displayed on the gaming device.

(e) If approved before July 1, 2004, receive a waiver from the chairman for any modification to the device if the full implementation of this section can not be met. The chairman may waive portions of this section if the manufacturer can demonstrate to the chairman's satisfaction that the imposition of the full standard would hinder the design of the device or pose a hardship due to limitations in the approved platform.

3. Any gaming device executing control programs from electrically erasable or volatile memory must employ a mechanism approved by the chairman that ensures the integrity of all control program components residing therein, including fixed data and graphic information and

ensures that they are authentic copies of the approved components. Additionally, control program components, excluding graphics and sound components, must be fully verified at the time of loading into the electrically erasable or volatile memory and upon any significant event, including but not limited to game resets and power up. The mechanism must prevent further play of the gaming device if an invalid component is detected.

4. Unless otherwise approved by the chairman, any gaming device that allows the adding, removing, or alteration of any control program components through a data communication facility must employ a mechanism for:

(a) Preventing any change from taking place that would interrupt a game in progress or a game session; and

(b) Storing program changes including changes in graphics and sound information in a non-volatile device that may be verified using such means as prescribed by the chairman.

Any device, technique or network which may be used to accomplish the adding, removing, or alteration of any control program components may, at the chairman's discretion, be considered a gaming device that must receive separate commission approval.

5. Gaming devices with control programs or other security programs residing in conventional Read Only Memory (ROM) devices such as EPROM's or fusible-link PROM's must have the unused portions of the memory device that contains the program set to zero.

6. Gaming device control programs must check for any corruption of random access memory locations used for crucial gaming device functions including, but not limited to, information pertaining to the play and final outcome of the most recent game, the nine games prior to the most recent game, random number generator outcome, credits available for play, and any error states. These memory areas must be checked for corruption following game initiation but prior to display of the game outcome to the player. Detection of any corruption that cannot be corrected shall be deemed to be a game malfunction and must result in a tilt condition.

7. All gaming devices must have the capacity to display a complete play history for the most recent game played and nine games prior to the most recent game. Retention of play history for additional prior games is encouraged. The display must indicate the game outcome (or a representative equivalent), intermediate play steps (such as a hold and draw sequence or a double-down sequence), credits available, bets placed, credits or coins paid, and credits cashed out. Gaming devices offering games with a variable number of intermediate play steps per game may satisfy this requirement by providing the capability to display the last 50 play steps.

Note: In accordance with this standard, 10 games (nine prior and the most recent) must be stored in memory. In games where "free games" are awarded as the result of a qualifying alignment, the "free games" are regarded as intermediate play steps of the game that initially awarded the free games. As such, the initiating game and the last 50 free games awarded must be stored in game memory. For games that award additional "free games" during free game play, the subsequent "free game" initiating games need not be stored unless they are contained in the last 50 free games played.

8. All gaming devices must have the capacity to display a complete transaction history for the most recent transaction with a cashless wagering system, and the previous thirty-four transactions prior to the most recent transaction, that incremented any of the in-meters set forth in Technical Standard 2.040(1)(i) through (t) and that incremented any of the out-meters set forth in Technical Standard 2.040(1)(i) through (t). Retention of transaction history for additional prior transactions is encouraged. (Amended: 8/8/11)

#### **1.084 Control Program Requirements for System Supported Games.**

1. Conventional gaming devices or clients that are considered part of a system supported gaming device containing control programs must comply with the requirements of Technical Standard 1.080.

2. Systems must be capable of verifying that all control programs contained on the server or system portion are authentic copies of approved components both automatically at least once every 24 hours and on demand. The authentication mechanism must employ a hashing algorithm which produces a message digest output of a least 128 bits. If the message digest is stored on a memory device other than a Conventional ROM Device the digest must be encrypted using a public/private key algorithm with a minimum of a 512 bit key or must be a bit-for-bit comparison. The mechanism

must prevent the execution of any control program component if the component is determined to be invalid. If an error(s) is detected, the system must provide a visual notification of the invalid program. Any program component of the authentication mechanism must reside on and securely load from non-alterable media. A report shall be available which details the outcome of each automated execution of the authentication mechanism and shall identify any invalid program components.

3. The system or server portion of the system supported game must provide, as a minimum, a two-stage mechanism for verifying all program components on demand via a communication port and protocol approved by the Chairman. The mechanism must employ a hashing algorithm which produces a message digest output of a least 128 bits and must be designed to accept a user selected authentication key or seed to be used as part of the mechanism (i.e. HMAC SHA-1). The first stage of this mechanism must allow for verification of all control components. The second stage must allow for verification of all program components, including graphics and data components in a maximum of 20 minutes. The system or server portion must also provide the same two-stage mechanism for verifying all program components on demand via a user interface where the results are displayed on the user interface.

4. System supported games shall be configured such that the system administrator level access may not be achieved without the presence and participation of at least two individuals. This may include split passwords, dual keys or any other suitable method approved by the chairman.

5. System supported games must provide a log entry anytime an individual causes a software component to be added, removed or altered in the server or system portion of the device. Each log entry must contain the date and time of the action, identification of the component affected, the identification of the individual performing the modification, the reason for the modification and any pertinent authentication information. This log must be maintained on the server or system portion of the device as well as on a computer or other logging device not accessible to the individual making the program modification that resides outside the secure area where the server or system component of the device resides. The record of the control program changes must be maintained for at least 90 days. A system supported game is not required to log this information on the secondary logging device if the information has been rendered unalterable, through a means approved by the Chairman, on the server or system part of the gaming device.

6. A log entry must be made on the conventional gaming device or client, on the server or system portion of the device and on a computer or other logging device residing outside of the secure area that houses the system supported game anytime a change is made to the software, to include control programs, data, graphics or sound information, in a connected conventional gaming device or client. Each log entry must contain the date and time of the action, identification of the component affected, the reason for the modification, and any pertinent authentication information. This information must be retained on the server or system portion of the game and on the secondary logging device for a minimum of 90 days. The conventional gaming device or client station must retain the listed information for at least 100 downloads. A system supported game is not required to log this information on the secondary logging device if the information has been rendered unalterable, through a means approved by the Chairman, on the server or system part of the gaming device.

7. Conventional gaming devices or clients that form a part of a system supported game must employ a mechanism that ensures that software downloaded to the conventional gaming device or client from the server or system portion of the system supported game is authentic and is received completely and without modification.

8. The server or system portion of a system supported game must authenticate any software downloaded to a connected conventional gaming device or client. The authentication information must support a resolution of at least 128 bits. The system supported game must support a command(s) that causes any conventional gaming device or client to authenticate any software downloaded from the server or system portion of the gaming device and must be able to disable the conventional gaming device or client if the authentication response is incorrect. Additionally, if the authentication response is not correct, a suitable tilt message must be displayed on the conventional gaming device or client station and a notification must be displayed on the server portion of the system supported game.

9. A system supported game must not alter any component of the system or server portion or the conventional gaming device or client portion of the device that would interrupt, or affect the function or operating parameters of a game in progress on any conventional gaming device or client station.



10. If a system supported game downloads software components to a conventional gaming device or client station, the downloaded software must be completely authenticated prior to performing any operation on the software including, but not limited to, decrypting, extracting or uncompressing. The downloaded software may not be applied or made available for play until such time as the conventional gaming device or client has met the conditions for changing the active software.

11. A system supported game must have the capacity to display a complete game play history for the most recent game and at the least 9 games prior to the most recent for each conventional gaming device or client station. The display of the play history for each individual client station or conventional gaming device must be available at the particular client station or conventional gaming device. The display must indicate the game outcome, intermediate play steps (such as a hold/draw sequence or individual bonus game choices), credits available, bets placed, credits or coins paid, and credits cashed out. Gaming devices offering games with a variable number of intermediate play steps per game may satisfy this requirement by providing the capability to display the last 50 play steps. The requirement to display game recall applies to all game programs currently installed on the conventional gaming device or client station.

(Adopted: 11/17/05. Amended: 8/8/11)

### **1.086 Control Program Requirements for System Based Games.**

1. Conventional games or clients that are considered part of a system based game containing control programs must comply with the requirements of Technical Standard 1.080.

2. System based games must be capable of verifying that all control programs contained on the server or system portion are authentic copies of approved components of the gaming device both automatically, at least once every 24 hours, and on demand. The authentication mechanism must employ a hashing algorithm which produces a messages digest output of a least 128 bits. If the message digest is stored on a memory device other than a Conventional ROM Device the digest must be encrypted using a public/private key algorithm with a minimum of a 512 bit key or must be a bit-for-bit comparison. The mechanism must prevent the execution of any control program component if the component is determined to be invalid. Any program component of the authentication mechanism must reside on and securely load from non-alterable storage media. A report shall be available which details the outcome of each automated execution of the authentication mechanism and shall identify any program components determined to be invalid.

3. System based games must provide for a secondary verification method based on a user input seed of at least 32 bits. The verification method will return a verification result of at least 32 bits corresponding to the control programs currently installed in the system or server portion of the device as well as the client or conventional portion of the gaming device.

4. System based games shall be configured such that system administrator level access may not be achieved without the presence and participation of at least two individuals. This may include split passwords, dual keys or any other suitable method approved by the chairman.

5. System based games must provide a log entry anytime an individual causes a software component to be added, removed or altered in the server or system portion of the device. Each log entry must contain the date and time of the action, identification of the component affected, identification of the individual performing the modification, the reason for the modification and any pertinent authentication information. This log must be maintained on the server or system portion of the device as well as on a computer or other logging device, not accessible to the individual making the program modification, that resides outside the secure area where the server or system component of the device resides. The record of the control program changes must be maintained for at least 90 days. A system based game is not required to log this information on the secondary logging device if the information has been rendered unalterable, through a means approved by the Chairman, on the server or system part of the gaming device.

6. System based games must provide a log entry on the server or system portion of the device and on a computer or other logging device residing outside of the secure area that houses the server or system portion of the device anytime the server or system portion of the game causes a change in the software to include control programs, data, graphics or sound information in the connected conventional gaming device or client. The record must contain the date and time of the action, identification of the component affected, the reason for the modification, and any pertinent authentication information, and must be maintained for a minimum of 90 days. A system based

game is not required to log this information on the secondary logging device if the information has been rendered unalterable, through a means approved by the Chairman, on the server or system part of the gaming device.

7. Conventional gaming devices or clients that form a part of a system based game must employ a mechanism that ensures that any software downloaded to the conventional gaming device or client from the server or system portion of the system based game is authentic, and is received completely and without modification.

8. The server or system portion of a system based game must authenticate any software downloaded to a connected conventional gaming device or client. The authentication information must support a minimum resolution of at least 128 bits. The system based game must support a command(s) that causes any conventional gaming device or client to authenticate any software downloaded from the server or system portion of the gaming device and must be able to disable the conventional gaming device or client if the authentication response is incorrect. Additionally, if the authentication response is not correct a suitable tilt message must be displayed on the conventional gaming device or client station and a notification must be displayed on the server portion of the system based game.

9. System based games must have the capacity to display a complete play history for the most recent game played and at least 34 games prior to the most recent game for each client station connected to the system based game. The display must indicate the game outcome (or a representative equivalent), intermediate play steps (such as hold and draw sequence or a double-down sequence), credits available, bets placed, credits or coins paid, and credits cashed out. Gaming devices offering games with a variable number of intermediate play steps per game may satisfy this requirement by providing the capability to display the last 50 play steps. The capability to initiate game recall must be available at the client for recall of information specifically associated with the particular client station initiating the game recall. The capacity to initiate game recall for any and all clients that make up the system based game must be available from the system or server portion of the system based gaming device. The requirement to display game recall applies to all game programs currently installed on the server portion of the system based game.

10. All system based games must have the capacity to display a complete transaction history for transactions with a cashless wagering system to include the most recent and the previous thirty-four transactions prior to the most recent transaction for each client station and the previous 99 transactions for the overall gaming device, that incremented any of the in-meters set forth in Technical Standard 2.040(1) (i) through (t) and that incremented any of the out-meters set forth in Technical Standard 2.040(1) (i) through (t). The capacity to initiate transaction history must be available at the client or conventional gaming device for the transaction history specifically associated with the particular client station initiating the history information request. The capacity to initiate a display of a transaction history for any and all clients or conventional gaming devices that make up the system based game must be available from the system or server portion of the system based game.

11. A system based game must not alter any component of the system or server portion or the conventional gaming device or client portion of the device that would interrupt, or affect the function or operating parameters of a game in progress at any conventional gaming device or client station.

12. If a system based game downloads software components to a conventional gaming device or client station, the downloaded software must be authenticated immediately upon receipt by the conventional gaming device or client station. The downloaded software may not be applied or made available for play until such time as the conventional gaming device or client has successfully authenticated the downloaded software, and has met the conditions for changing the active software.

13. A system based game must provide a secure interface port through which the software on the system and client portions of the game may be authenticated.

(Adopted: 11/17/05. Amended: 8/8/11)

**1.090 Bonus or Extended Game Features.** All gaming devices which offer a bonus game or extended feature which requires player selection or interaction are prohibited from automatically making selections or initiating games or features unless the gaming device meets one of the following requirements and explains the mechanism for auto-initiation or selection on the device glass or video display.

1. The patron is presented with a choice and specifically acknowledges his intent to have the gaming device auto-initiate the bonus or extended play feature by means of a button press or other physical/machine interaction.

2. The bonus or extended feature provides only one choice to the patron i.e., press button to spin wheel. In this case, the device may auto initiate the bonus or extended feature after a time out period of at least 2 minutes.

3. The bonus or extended feature is offered as part of community play that involves two or more patrons and where the delay of an offered selection or game initiation will directly impact the ability for other patrons to continue their bonus or extended feature. Prior to automatically making selections or initiating a community based bonus or feature the patron must be made aware of the time remaining in which they must make their selection or initiate play.

(Adopted: 12/04. Amended: 8/8/11)

#### **1.100 Reel strips.**

1. Given a physical reel strip of length L units containing N physical stops, each blank space must occupy a minimum of  $(L/N)*0.4$  units. These blank symbols must be completely free of any portion of any adjacent symbol.

2. All non-blank and blank symbols must be centered in their respective space allocation.

(Adopted: 12/04. Effective: 1/1/05)

#### **1.110 Safety.**

1. A gaming device must not present a mechanical, electrical or fire hazard when used in its intended mode of operation.

2. The power supply used in a gaming device must be designed to minimize leakage current in the event of intentional or inadvertent disconnection of the AC power ground. Leakage currents of greater than 1.0 milliamperes may be considered hazardous. The power supply must be appropriately fused or protected by circuit breakers. [\*A manufacturer may request a waiver from the chairman of the requirements of this section for gaming devices that are certified by an OSHA Nationally Recognized Testing Laboratory for safety.\*](#)

(Adopted: 9/89. Amended: 1/1/05)

#### **1.120 System Based Game Configuration.**

1. A system based game, with more than 64 client stations, must be configured such that a failure of any single part or piece of equipment or a failure of the system based game's automated software authentication will not result in a cessation of operation of the system based game.

2. A system based game, with more than 64 client stations, must be configured such that a failure of any single part or piece of equipment will not result in more than 50% of the associated client stations being disabled.

3. A system based game must be configured such that a failure of any single part or piece of equipment will not result in any stored information regarding game recall, cashless wagering transaction history, or game performance and accounting being lost or destroyed.

4. A client must be rendered unplayable if communications from the server or system portion of the gaming device is lost. However, in the case of clients that have lost communications with the server, the client must provide a means, such as a hand pay, for patrons to cash out credits indicated on the system based gaming device at the time the communications was lost.

(Adopted: 11/17/05. Amended: 8/8/11)

#### **1.130 Requirements for downloading software to a conventional gaming device or client station from a system supported game.**

1. Prior to any software being added or removed from a conventional gaming device or client station comprising a part of a system supported game that would result in the loss of accounting meter information, a complete set of meter information to include all meters required by Technical Standard 2.040 must be successfully communicated to a slot accounting system.

2. Software may not be added onto or removed from a conventional gaming device or client station if an error or tilt condition exists on the conventional gaming device or client station.

(Adopted: 11/17/05)

### **1.135 Requirements for downloading software to a conventional gaming device or client station from a system based game.**

1. Prior to any software being added or removed from a system based game that would result in the loss of accounting meter information, a complete set of meter information to include all the meters required by Technical Standard 2.040 for all the client stations as well as the system must be successfully communicated to a slot accounting system.

2. Software may not be removed from a system based game if the particular software being removed is being served to a client station that is in an error or tilt condition.

(Adopted: 11/17/05)

### **1.140 Conditions for changing active software on a conventional gaming device or client station that is part of a system supported or system based game.**

1. Active software consists of all the games currently available for immediate play by the patron on the conventional gaming device or client station. For this section, immediate play means games that do not require additional software or a change in game configuration such as denomination, maximum wager, payback percentage, etc. prior to the patron being able to initiate play. Active software also includes any software in which a change will interrupt normal game play, i.e. game operating system and peripheral firmware.

2. The conventional gaming device or client station must:

(a) Be in the idle mode with no errors or tilts, no play and no credits on the machine for at least ~~4~~ two (2) minutes;

(b) Not be participating in an in-house or inter-casino linked payoff schedule where the change will result in a violation of Regulation 5.110 or 5.112; and

~~[(c) Be disabled and rendered unplayable for at least 4 minutes following the change in active software. During the time the machine is disabled a message must be displayed on a video screen or other appropriate display device notifying the patron that the game configuration has been changed.]~~

3. If the change in the active software is the direct result of a player request or a qualifying event that is not an identifier, the time delay requirements of section 2(a) of this technical standard may be ignored. However, the active software may not be changed if an error or tilt exists on the conventional gaming device or client station.

Note: A qualifying event may include, but is not limited to, the number of games played or the cumulative amount wagered by a patron during a gaming session as provided for in the rules of play.

(Adopted: 11/17/05. Amended: 8/8/11)

### **1.200 Logging Requirements for the use of Identifiers**

1. A system based game, system supported game, or gaming associated equipment that assigns or tracks the use of identifiers must log the following information on the system component each time an identifier is assigned:

- (a) A transaction identification number unique to the assignment;
- (b) The transaction date and time;
- (c) An identification number unique to the patron, if known;
- (d) The category or name of the identifier assigned;
- (e) The basis for the assignment of the identifier; and
- (f) Any other information necessary to reconcile the assignment of an identifier to a patron.

2. The logged information required by Technical Standard 1.200 (1) must:

- (a) Be retained for a minimum of 30 days;
- (b) Be viewable on the system portion of the gaming device;
- (c) Be exportable into a comma separated values text file; and
- (d) Be rendered unalterable using a method approved by the chairman.

3. A conventional gaming device or client of a system supported gaming device that uses identifiers must log the following information each time an identifier is used:

- (a) A transaction identification number unique to the assignment or the transaction identification number assigned by the system component or associated equipment;
- (b) The transaction date and time;
- (c) The category or name of the identifier assigned; and
- (d) The basis for the assignment of the identifier, if assigned by the conventional gaming device or client of a system supported gaming device.

This information must be maintained for at least the most recent ten identifiers assigned and must be displayable on the conventional gaming device or client of a system supported gaming device.

4. As used in this technical standard, the basis for the assignment of an identifier include, without limitation, one or more of the following:

- (a) The frequency, value or extent of predefined commercial activity such as the patron's frequency of visitation or wagering activity at a licensee(s); activity on social media; or accumulation of rank, points, or standing in either gaming or non-gaming activity;
- (b) The subscription to or enrollment in particular services such as membership in a licensee's customer loyalty program;
- (c) The use of a particular technology concurrent with the play of a game;
- (d) The level of skill of a patron as identified or maintained by the gaming system or self-identified by the patron;
- (e) The level of skill of a patron relative to the skill of other patrons participating in the same game; or
- (f) The degree of skill required by the game.

### **1.300 Gaming devices that incorporate skill.**

1. A gaming device that incorporates skill and makes use of player interaction technology must:

- (a) Monitor the player interaction technology for proper operation before the initiation of each game. Upon detection of improper operation, the gaming device must enter into a tilt condition;
- (b) Provide a mechanism to calibrate the technology;

(c) Prevent unintended perturbations, such as physical, radio-frequency, or optical from impacting the proper operation of the game;

(d) Upon initialization, must automatically verify that it meets the minimum hardware requirements necessary to properly conduct the game. The gaming device must prevent initialization if the hardware is found to be insufficient; and

(e) Ensure that variances in hardware that meet the minimum hardware requirements, such as processing power, amount of memory, or data bandwidth available do not:

(1) Impact the proper operation of the game; or

(2) Provide an advantage or disadvantage to a player.

Note: This standard applies to the total amount of resources available to the gaming device. Manufacturers are encouraged to additionally monitor available resource levels during operation to ensure continued proper game play.

2. Hardware necessary to implement a game must be equivalent on each gaming device. Hardware variances must not:

(a) Impact the proper operation of the game; or

(b) Provide an advantage or disadvantage to a player.

Note: This standard applies to the total amount of resources available to the gaming device. Manufacturers are encouraged to additionally monitor available resource levels during operation to ensure continued proper game play.

3. For each enabled payable, the gaming device must calculate the actual payback percentage every N games, where N is the number of games necessary to determine the theoretical payback percentage with a 95% confidence interval within a range of +/- 5%. The device shall:

(a) Determine the absolute value of the difference between the actual payback percentage and the theoretical payback percentage;

(b) Maintain a record of the most recent 50 calculations for each payable to include the date, time, payable ID, the calculated actual payback percentage and the absolute value of the difference between the actual payback percentage and the theoretical payback percentage; and

(c) Upon detection of three consecutive calculations, for a payable, in which the absolute value of the difference between the actual and theoretical payback percentages is greater than 4%, enter into a tilt condition.

4. The rules of play for a game of skill or hybrid game must describe or display information adequate for a reasonable person to understand the method of game play prior to the player committing a wager.

(a) The content of the rules of play necessary to comply with this subsection will be determined based on an evaluation of the following factors:

(1) The theme of the game;

(2) Knowledge of the game among the general public based on the history and prevalence of the game or readily identifiable variations of the game;

(3) The extent to which the format of the game differs from that of a substantially comparable game known in contexts outside the casino gaming environment; and

(4) The physical attributes of the game, including whether the game is based on:

(i) Inherent skill based on physical dexterity, endurance and strategy, such as in an athletic activity;

(ii) Skill based on expertise, education or experience, such as a word or trivia contest; and

(iii) Dynamic skill based on variations in the difficulty or complexity of a skill activity that change in response to the player's decisions, acuity, agility, dexterity, game duration or an inherent game feature, such as a military combat game.

(b) The rules of play may be communicated to the player singularly or through a combination of:

(1) The rules or descriptions displayed by the gaming device;

(2) The pay table; or

(3) A game tutorial or demonstration displayed by the gaming device or at a prominently disclosed location within the gaming establishment.

#### **1.400 Random Selection Process and Random Number Generator**

1. The random selection process must meet 95 percent confidence limits using a standard chi-squared test for goodness of fit.

2. A gaming device using a software random number generator (RNG) shall:

(a) Not use static seed upon initialization;

(b) Cycle the RNG at a minimum average rate of 100Hz (100 times per second); and

(c) Not draw RNG values for future play.

3. A gaming device using a hardware random number generator shall:

(a) Continually monitor the RNG to ensure compliance with this standard. This shall be done by performing a chi-squared goodness of fit evaluation over the most recent 10,000 random outcomes selected for game play;

(b) Automatically maintain an event log displaying the results of the most recent 10 chi-squared tests to include the result of the test and the date and time the test was performed;

(c) Display a visual indicator of a failure; and

(d) Upon, two consecutive failures, enter into a tilt condition.

4. RNG's used for purposes other than determining the game outcome must either:

(a) Be implemented as a separate instantiation of the RNG process; or

(b) Be based on an algorithm or method that can be demonstrated does not affect the game outcome.

5. A game that draws a predetermined set of outcomes for a game, such as a shuffled deck of cards, must prevent the information from being accessible.

6. Additionally, video poker games must not determine replacement cards prior to the player selecting hold cards and initiating a draw.

7. The RNG and random selection process must be impervious to influences from outside the device, including, but not limited to, electro-magnetic interference, electro-static interference, and radio frequency interference.

8. A gaming device must use appropriate communication protocols to protect the random number generator and random selection process from influence by associated equipment or other devices which is conducting data communications with the gaming device.

**End – Technical Standard 1**