

TECHNICAL STANDARDS FOR GAMING DEVICES AND ON-LINE SLOT SYSTEMS

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. ~~Logical~~ **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. ~~Logical~~ **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 90 days.

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

1.066 Remote access to gaming devices. Remote access includes all access to the 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 non-administrative functions which excludes the following activities:

(a) Configuration of the operating system;

(b) The addition or deletion or modification of server or system files;

(c) The execution of non SSG/SBG applications;

(d) Executing or halting system services; and

(e) Shutting down or restarting the server(s).

32. A system supported or system based game must be **securely** isolated from any remote access connection by ~~at least two different firewalls~~ **through a means approved by the Chairman**. ~~At least one of the firewalls must be a hardware implementation.~~

43. A system supported or system based game 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.

54. A system based or system supported game must provide a hardware or software mechanism that will sever the connection between the gaming device and the remote access terminal. 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.

65. A system supported or system based game 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.

76. A system supported or 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.

87. **If a system based or system supported gaming device allows for downloading of new gaming device applications or gaming device related firmware through remote access, the s**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.

98. If a system based or system supported gaming device allows for downloading of new gaming device applications or gaming device related firmware through remote access, the sSoftware 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 or uncompressing.

(Adopted: 11/17/05.)

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 chairman may require tests to verify that components used by Nevada licensees are approved components. The verification mechanism must have an error rate of less than 1 in 10 to the 38th power and must prevent the execution of any control program component if any component is determined to be invalid. Any program component of the verification or 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 validation information.

(d) Provide, as a minimum, a two-stage mechanism for validating all program components on demand via a communication port and protocol approved by the chairman. The first stage of this mechanism must verify all control components. The second stage must be capable of completely authenticating all program components, including graphics and data components in a maximum of 20 minutes. The mechanism for extracting the authentication information must be

stored on a Conventional ROM Device that must be capable of being authenticated by a method approved by the chairman. **[Effective 1/1/09] All gaming devices must also provide the same two-stage mechanism for validating 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.

8. **[Effective 2/1/04]** 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 (s) and that incremented any of the out-meters set forth in Technical Standard 2.040(1)(i) through (s). Retention of transaction history for additional prior transactions is encouraged.

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 method of validation must provide at least 128 bits of resolution or must be a bit-for-bit comparison and 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 verification 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 validation mechanism and shall identify any invalid program components.

3. System supported 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.

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 validation 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 validation 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 validate any software downloaded to a connected conventional gaming device or client. The validation 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 validate 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 validation response is incorrect. Additionally, if the validation 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 provide a secure interface port through which the software on the system portion of the game may be authenticated and validated.

12. 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.)

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 method of validation must provide at least 128 bits of resolution or must be a bit-for-bit comparison and must prevent the execution of any control program component if the component is determined to be invalid and provide a visual notification of the invalid program. Any program component of the verification 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 validation 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 validation 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 validation 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 validate any software downloaded to a connected conventional gaming device or client. The validation 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 validate 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 validation response is incorrect. Additionally, if the validation 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 (s) and that incremented any of the out-meters set forth in Technical Standard 2.040(1) (i) through (s). The capability 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 and validated.