STANDARD SERIES

GLI-25:

Dealer Controlled Electronic Table Games

Version: 1.2

Release Date: September 6, 2011

This Page Intentionally Left Blank

ABOUT THIS STANDARD

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

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

Table of Contents

CHAPTER 1
1.0 STANDARD OVERVIEW

1.1 Introduction

1.1.1 General Statement. **Gaming Laboratories International, LLC (GLI)** has been testing gaming equipment since 1989. Over the years, we have developed numerous standards for jurisdictions all over the world. In recent years, many jurisdictions have opted to ask for the development of industry standards without creating their own standards documents. In addition, with technology changing almost monthly, new technology is not being incorporated quickly enough into existing standards due to the long process of administrative rulemaking. This document, *GLI Standard 25*, will set forth the technical Standards for Dealer Controlled Electronic Table Games (ETG).

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

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

1.2 Purpose of Technical Standards

1.2.1 ***General Statement***. The Purpose of this Technical Standard is as follows:

a) To eliminate subjective criteria in analyzing and certifying Dealer Controlled Electronic Table Games.

b) To only test those criteria that impact the credibility and integrity of Dealer Controlled Electronic Table Games from both the Revenue Collection and Player's perspective.

c) To create a standard that will ensure that the Dealer Controlled Electronic Table Games are fair, secure, and able to be audited and operated correctly.

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

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

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

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

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

1.3 Other Documents That May Apply

1.3.1 General Statement. The following other GLI standards may apply, depending on the features of the electronic table game and references throughout this document. All GLI standards are available on our website at www.gaminglabs.com:

a) GLI-11 Gaming Devices in Casinos;
b) GLI-12 Progressive Gaming Devices in Casinos;
c) GLI-13 On-Line Monitoring and Control Systems (MCS) and Validation Systems in Casinos;
d) GLI-16 Cashless Systems in Casinos;
e) GLI-17 Bonusing Systems in Casinos; and
f) GLI-18 Promotional Systems in Casinos.

NOTE: This standard covers the Technical Specifications of the operation of Dealer Controlled Electronic Table Games, as defined within section 1.4.1 below, where the table games are operated electronically, that require interaction from a live dealer. Please refer to GLI-24 for Electronic Table Game Systems that do not utilize a live dealer.

1.4 Defining Dealer Controlled Electronic Table Games

1.4.1 General Statement. Dealer Controlled Electronic Table Games (ETG) is the operation of a table game(s) that require a live dealer that utilizes electronics as part of the game's operation (i.e., game generation, electronically collecting, storing, communicating accounting and significant event data, etc.) **This standard is only to be used when the electronic table game requires a live dealer. This standard will not make assumptions as to the classification of a device in a particular jurisdiction as being a table game or a gaming device, as defined within the GLI-11 Gaming Devices in Casinos standard. Nor does GLI offer an opinion as to how many 'devices' the equipment encompasses.**

NOTE: For table game systems that do not utilize a live dealer please refer to the GLI Standard 24.

1.5 Phases of Testing

1.5.1 ***General Statement***. Electronic table game submissions to the Test Laboratory may be performed in two phases:

a) Within the laboratory setting; and
b) On-site following the initial install of the system to ensure proper configuration of the security applications.

NOTE: In addition to the on-site testing of the system, the Test Laboratory shall provide training on this new technology to the local regulators, recommended field auditing procedures, and assistance with the compilation of Internal Controls, if requested.

CHAPTER 2

2.0 ELECTRONIC TABLE GAME SYSTEM REQUIREMENTS

2.1 Introduction

This chapter addresses electronic table game's that may or may not function as a component within a table game system. The regulations of each subchapter only apply when the electronic table game(s) operate as part of a 'table game system' that is independent of any external gaming system. Electronic table game's that operate in conjunction with external systems shall meet the game level and communication requirements established within the appropriate GLI Standard.

2.2 Table Game System Requirements

2.2.1 ***System Clock***. The system must maintain an internal clock that reflects the current time (24hr format - which is understood by the local date/time format) and date that shall be used to provide for the following:

a) Time stamping of significant events;
b) Reference clock for reporting; and
c) Time stamping of configuration changes.

2.2.2 ***Synchronization Feature***. If multiple clocks are supported the system shall have a facility whereby it is able to synchronize those clocks in each system component, whereby conflicting information could not occur.

2.3 System Security

2.3.1 ***General Statement***. All communications, including Remote Access, must pass through at least one approved application-level firewall and must not have a facility that allows for an alternate network path.

2.3.2 ***Firewall Audit Logs***. The firewall application must maintain an audit log of the following information and must disable all communications and generate an error event if the audit log becomes full:

a) All changes to configuration of the firewall;
b) All successful and unsuccessful connection attempts through the firewall; and
c) The source and destination IP Addresses, Port Numbers and MAC Addresses.

2.3.3 ***Surveillance/Security Functionality***. The system shall provide for interrogation that enables on-line comprehensive searching of the significant event log.

2.3.4 ***Access Control***. The system must support either a hierarchical role structure whereby user name and password define program access or individual menu item access or logon program /device security based strictly on user name and password or PIN. The system shall not permit the alteration of any significant log information without supervised access control. There shall be a provision for system administrator notification and user lockout or audit trail entry, after a set number of unsuccessful login attempts. The system shall record: Date and Time of the Login attempt, username supplied, and success or failure. The use of generic user accounts on servers is not permitted.

2.3.5 ***Data Alteration***. The system shall not permit the alteration of any accounting or significant event log information without supervised access controls. In the event financial data is changed, an audit log must be capable of being produced to document:

a) Data element altered;

b) Data element value prior to alteration;
c) Data element value after alteration;
d) Time and Date of alteration; and
e) Personnel that performed alteration (user login).

2.4 Remote Access

2.4.1 ***Remote Access defined***. Remote access defines any access made by a component outside the 'trusted' network.

2.4.2 ***General Statement***. Remote access where permitted, shall authenticate all computer systems based on the authorized settings of the electronic table game and firewall application that establishes a connection with the electronic table game as long as the following requirements are met:

a) Remote Access User Activity log is maintained by both the property and the manufacturer, depicting: authorized by, purpose, logon name, time/date, duration, and activity while logged in;
b) No unauthorized remote user administration functionality (adding users, changing permissions, etc.);
c) No unauthorized access to database;
d) No unauthorized access to operating system; and
e) If remote access is to be on a continuous basis then a network filter (firewall) must be installed to protect access (Dependent upon jurisdictional approval).

2.4.3 ***Self Monitoring***. The system must implement self monitoring of all critical Interface Elements (e.g. central hosts, network devices, firewalls, links to third parties, etc.) and shall have the ability to effectively notify the system administrator of any error condition, provided the condition is not catastrophic. The system shall be able to perform this operation with a frequency of at least once in every 24-hour period and during each power-up and power reset.

2.5 Backups and Recovery

2.5.1 ***System Redundancy, Backup & Recovery***. The system shall have sufficient redundancy and modularity so that if any single component or part of a component fails, gaming can continue. There shall be redundant copies of each log file or system database or both on the system with open support for backups and restoration.

2.5.2 ***Backup & Recovery***. In the event of a catastrophic failure when the system cannot be restarted in any other way, it shall be possible to reload the system from the last viable backup point and fully recover the contents of that backup, recommended to consist of at least the following information:

a) Significant events;
b) Accounting information;
c) Auditing information; and
d) Specific site information such as Device file, Employee file, game profiles, etc.

2.6 Communication Protocol

2.6.1 ***General Statement***. Each component of an electronic table game system must function as indicated by the communication protocol implemented. All protocols must use communication techniques that have proper error detection and/or recovery mechanisms which are designed to prevent unauthorized access or tampering, employing Data Encryption Standards (DES) or equivalent encryption with secure seeds or algorithms. Any alternative measures will be reviewed on a case-by-case basis, with regulator approval.

2.7 System Integrity

2.7.1 General Statement. The Laboratory will perform certain tests to determine whether or not outside influences affect game fairness to the player or create cheating opportunities. This certification applies exclusively to tests conducted using current and retrospective methodology developed by Gaming Laboratories International, LLC (GLI). During the course of testing, GLI inspects for marks or symbols indicating that a device has undergone product safety compliance testing. Gaming Laboratories International, LLC also performs, where possible, a cursory review of submissions and information contained therein related to Electromagnetic Interference (EMI), Radio Frequency Interference (RFI), Magnetic Interference, Liquid Spills, Power Fluctuations and Environmental conditions. Electrostatic Discharge Testing is intended only to simulate techniques observed in the field being used to attempt to disrupt the integrity of electronic table game systems. Compliance to any such regulations related to the aforementioned testing is the sole responsibility of the device manufacturer. GLI claims no liability and makes no representations with respect to such non-gaming testing. An electronic table game system shall be able to withstand the following tests, resuming game play without operator intervention:

a) Random Number Generator. If implemented, the random number generator and random selection process shall be impervious to influences from outside the device, including, but not limited to, electro-magnetic interference, electro-static interference, and radio frequency interference;

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

2.7.2 ***Physical Security***. The server or system component(s) must reside in a secure area where access is limited to authorized personnel. It is recommended that logical access to the game be logged on the system or 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. The logged data should include the time, date, and the identity of the individual accessing the secure area. The resulting logs should be kept for a minimum of 90 days.

2.8 Random Number Generator

2.8.1 ***General Statement***. The Random Number Generator (RNG) is the selection of game symbols or production of game outcomes. The regulations within this section are only applicable to electronic table games that utilize an RNG, which shall:

a) Be statistically independent;
b) Conform to the desired random distribution;
c) Pass various recognized statistical tests; and
d) Be unpredictable.

2.8.2 ***Game Selection Process***.

a) All Combinations and Outcomes Shall Be Available. Each possible permutation or combination of game elements that produces winning or losing game outcomes shall be available for random selection at the initiation of each play, unless otherwise denoted by the game.
b) No Near Miss. After selection of the game outcome, the electronic table game shall not make a variable secondary decision, which affects the result shown to the player. For instance, the random number generator chooses an outcome that the game will be a loser.
c) No Corruption from Associated Equipment. An electronic table game shall use appropriate protocols that effectively protect the random number generator and random

selection process from influence by associated equipment, which may be communicating with the electronic table game.

2.8.3 Applied Tests. The test laboratory may employ the use of various recognized tests to determine whether or not the random values produced by the random number generator pass the desired confidence level of 99%. These tests may include, but are not limited to:

a) Chi-square test;
b) Equi-distribution (frequency) test;
c) Gap test;
d) Overlaps test;
e) Poker test;
f) Coupon collector's test;
g) Permutation test;
h) Kolmogorov-Smirnov test;
i) Adjacency criterion tests;
j) Order statistic test;
k) Runs tests (patterns of occurrences should not be recurrent);
l) Interplay correlation test;
m) Serial correlation test potency and degree of serial correlation (outcomes should be independent of the previous game);
n) Tests on subsequences; and
o) Poisson distribution.

2.8.4 Background RNG Activity. The RNG shall be cycled continuously in the background between games and during game play at a speed that cannot be timed by the player. The test laboratory recognizes that some time during the game, the RNG may not be cycled when interrupts may be suspended. The test laboratory recognizes this but shall find that this exception shall be kept to a minimum.

2.8.5 ***RNG Seeding***. The first seed shall be randomly determined by an uncontrolled event. After every game there shall be a random change in the RNG process (new seed, random timer, delay, etc.). This will verify the RNG doesn't start at the same value, every time. It is permissible not to use a random seed; however, the manufacturer must ensure that games will not synchronize.

2.8.6 ***Live Game Correlation***. Unless otherwise denoted on the pay glass/display, where the electronic table game plays a game that is recognizable such as Poker, Blackjack, Roulette, etc., the same probabilities associated with the live game shall be evident in the simulated game. For example, the odds of getting any particular number in Roulette where there is a single zero (0) and a double zero (00) on the wheel, shall be 1 in 38; the odds of drawing a specific card or cards in Poker shall be the same as in the live game.

2.8.7 ***Card Games***. The requirements for games depicting cards being drawn from a deck are the following:

a) At the start of each game/hand, the cards shall be drawn fairly from a randomly-shuffled deck; the replacement cards shall not be drawn until needed, and in accordance with game rules, to allow for multi-deck and depleting decks;
b) Cards once removed from the deck shall not be returned to the deck except as provided by the rules of the game depicted;
c) As cards are removed from the deck they shall be immediately used as directed by the rules of the game (i.e., the cards are not to be discarded due to adaptive behavior by the electronic table game system)

NOTE: It is acceptable to draw ***random numbers*** *for replacement cards at the time of the first hand random number draw. Provided the replacement cards are sequentially used as needed.*

2.9 Maintenance of Critical Memory

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

Note: The "Maintenance of Critical Memory" section is not intended to preclude the use of alternate storage media types, such as hard disk drives, for the retention of critical data. Such alternate storage media is still expected to maintain critical data integrity in a manner consistent with the requirements in this section, as applicable to the specific storage technology implemented.

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

2.9.3 Unrecoverable Critical Memory. An unrecoverable corruption of critical memory shall result in an error. The memory error shall not be cleared automatically and shall result in a tilt condition, which facilitates the identification of the error and causes the electronic table game to cease further function. *The critical memory error shall also cause any communication external to the electronic table game to immediately cease.* An unrecoverable critical memory error shall require a full non-volatile memory clear performed by an authorized person.

2.9.4 Non-volatile Memory and Program Storage Device Space. Non-volatile memory space that is not critical to the electronic table game operations are not required to be validated.

2.10 Program Storage Device Requirements

2.10.1 General Statement. The term *Program Storage Device* is defined to be the media or an electronic device that contains the critical control program components. Device types include

but are not limited to EPROMs, compact flash cards, optical disks, hard drives, solid state drives, USB drives, etc. This partial list may change as storage technology evolves. All program storage devices shall:

a) Be housed within a fully enclosed and locked logic compartment;
b) Be clearly marked with sufficient information to identify the software and revision level of the information stored in the device. In the case of media types on which multiple programs may reside it is acceptable to display this information via the attendant menu.
c) Validate themselves during each processor reset;
d) Validate themselves the first time they are used; and
e) CD-ROM, DVD, and other optical disk-based Program Storage shall:
    i. Not be a re-writeable disk; and
    ii. The "Session" shall be closed to prevent any further writing.

2.11 Control Program Requirements

2.11.1 Control Program Verificatiom.

a) EPROM-based Program Storage:
    i. Electronic table games which have control programs residing in one or more EPROMs must employ a mechanism to verify control programs and data. The mechanism must use at a minimum a checksum; however, it is recommended that a Cyclic Redundancy Check (CRC) be used (at least 16-bit).
b) Non-EPROM Program Storage shall meet the following rules:
    i. The software shall provide a mechanism for the detection of unauthorized and corrupt software elements, upon any access, and subsequently prevent the execution or usage of those elements by the electronic table game. The mechanism must employ a hashing algorithm which produces a message digest output of at least 128 bits.

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

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

c) Alterable Media shall meet the following rules in addition to the requirements outlined in 2.11.1(b):

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

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

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

2.11.2 <u>Program Identification</u>. Program storage devices which do not have the ability to be modified while installed in the electronic table game during normal operation, shall be clearly marked with sufficient information to identify the software and revision level of the information stored in the devices.

2.11.3 Independent Control Program Verification. The system server(s) and each component of the electronic table game that would have an effect on the integrity of the electronic table game shall have the ability to allow for an independent integrity check of the device's software from an outside source and is required for all control programs that may affect the integrity of the game. This must be accomplished by being authenticated by a third-party device, which may be embedded within the game software (see NOTE below), by having an interface port for a third-party device to authenticate the media, or by allowing for removal of the media such that it can be verified externally. This integrity check will provide a means for field verification of the software to identify and validate the program. The test laboratory, prior to device approval, shall evaluate the integrity check method.

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

2.12 Player Interface Terminal Requirements

2.12.1 General Statement. Player interface terminals may either be a display mechanism where the system performs all operations of the game (Thin Client), or contain its own logic function in conjunction with the electronic table game system (Thick Client). In either case, the player interface terminal(s) must meet the hardware and software requirements outlined within each jurisdiction's applicable requirements for gaming devices, to ensure security and player safety. In the absence of these jurisdictional specific requirements, the GLI-11 requirements should be used.

NOTE: Requirements that cannot be met as a result of manual intervention performed by the live dealer must be addressed in operational procedures and submitted to the Test Laboratory.