RULES
OF
THE TENNESSEE SPORTS WAGERING ADVISORY COUNCIL

CHAPTER 1350-03
MINIMUM INTERNAL CONTROLS

TABLE OF CONTENTS

1350-03-.01	Applicability	1350-03-.08	AML and Regulatory Compliance Standards
1350-03-.02	General Standards	1350-03-.09	Types of Wagers Available
1350-03-.03	User Access Controls for All Interactive Sports Gaming Personnel	1350-03-.10	Third-Party Systems
1350-03-.04	Segregation of Duties	1350-03-.11	Prohibition on Wagers and Payouts to Minors
1350-03-.05	Risk Management Procedures	1350-03-.12	Information System Minimum Controls
1350-03-.06	Identifying and Reporting Fraud and Unusual and Suspicious Activities	1350-03-.13	Information System Audit Requirements
1350-03-.07	Prevention of Interactive Sports Gaming by Ineligible Bettors		

1350-03-.01 APPLICABILITY.

This Chapter contains Minimum Internal Controls Standards ("MICS") applicable to all Licensees. The purpose of this Chapter is to ensure all Licensees apply the same minimal due diligence to their Interactive Sports Gaming operations in the State of Tennessee, including procedures, administration, and accounting controls in order to maintain the integrity of sports wagering in the State of Tennessee and to protect the public interest. Compliance with this Chapter ensures that Licensees have appropriate security controls in place so that Players are not exposed to unnecessary risks when choosing to participate in Interactive Sports Gaming.

This Chapter shall be included in and made a part of any Licensee's Interactive Sports Gaming operations. This Chapter may be amended pursuant to T.C.A. § 4-49-106(b). Defined terms, unless otherwise noted, shall have the same meaning included in Rule 1350-01-.02.

Authority: *T.C.A. §§ 4-49-106, 4-49-110, 4-49-115, and 4-49-125.* ***Administrative History:*** *Emergency rules filed December 22, 2021 to become effective January 1, 2022; effective through June 30, 2022. New rules filed March 22, 2022; effective June 20, 2022.*

1350-03-.02 GENERAL STANDARDS.

The following controls are required for Licensees offering Interactive Sports Gaming:

(1) A Licensee shall receive approval from the Council of its internal controls for all aspects of Sports Gaming Systems prior to commencing operations, as well as any time a significant change is made thereafter. The internal controls shall be submitted to the Council as part of the License Application, and shall be approved by the Council prior to when the Licensee begins conducting Interactive Sports Gaming.

(2) The following list of items includes procedures and controls that must be a part of each Licensee's internal controls:

(a) Safeguarding assets and revenues, including maintaining reliable records relating to accounts, transactions, profits and losses, operations, and events;

(b) Safeguarding Sports Gaming Accounts;

(c) Requirements for internal and independent audits of Licensee;

(Rule 1350-03-.02, continued)

(d) User access controls for all Interactive Sports Gaming personnel;

(e) Segregation of duties among all Interactive Sports Gaming personnel;

(f) Automated and manual risk management procedures;

(g) Procedures for identifying and reporting fraud, Cheating, and Suspicious or Unusual Wagering Activity;

(h) Procedures for identifying and preventing Minors from engaging in Interactive Sports Gaming;

(i) Procedures to prevent wagering by Prohibited Participants;

(j) Description of AML compliance standards;

(k) Description of all types of Wagers available to be offered by the Sports Gaming System;

(l) Description of all integrated third-party systems;

(m) Description of all hardware and software applications that comprise the Sports Gaming System;

(n) Description and sources of data and information feeds and services, including, but not limited to, official data, odds and line monitoring services, integrity monitoring services, and risk management support;

(o) Controls ensuring regulatory compliance;

(p) A monitoring system utilizing software to identify irregularities in volume or odds and swings that could signal Suspicious Wagering Activities that should require further investigation;

(q) Suspicious Wagers over any threshold set by the Licensee; and

(r) Description of the method to prevent past posting (i.e., a Wager made outside of the Wager period).

(3) Changes to Sports Gaming Systems

(a) A Licensee shall maintain a change management log listing changes to its Sports Gaming System. A Licensee shall submit the log to the Executive Director on the 15th day following the close of each calendar quarter. The log shall list:

1. Date and time of change;

2. A description and reason for the change, including each required control program component affected. If the component being changed is a hardware component, include its physical location;

3. The name or other user ID of the individual responsible for authorizing and/or conducting the change;

4. The Council approval date, if applicable;

5. The level of the change (Level 1, 2, or 3); and

6. The recording of the new digital signature for any change to a regulated control program component.

(b) Classification of changes:

1. Level 1 – No Impact: This change has no impact to regulated components of the Sports Gaming System. A Licensee shall report Level 1 changes as part of the quarterly change management log submission.

2. Level 2 – Low Impact: This change has a low impact on the integrity of the Sports Gaming System, including hardware component changes. A Licensee shall report Level 2 changes to the Executive Director at least five (5) business days in advance of the proposed implementation. The Executive Director may request more information or a pause in implementation if there are concerns.

3. Level 3 – High Impact: This change has a high impact on regulated components of the Sports Gaming System. A Licensee shall obtain prior written approval from the Executive Director or designee for Level 3 changes. A Licensee shall submit a request for a Level 3 change to the Executive Director for review and approval at least ten (10) business days in advance of the proposed implementation. The Licensee may deploy the update only after receiving written approval from the Executive Director or designee.

Authority: *T.C.A. §§ 4-49-106, 4-49-110, 4-49-111, 4-49-112, 4-49-115, 4-49-117, 4-49-122, and 4-49-125.* ***Administrative History:*** *Emergency rules filed December 22, 2021 to become effective January 1, 2022; effective through June 30, 2022. New rules filed March 22, 2022; effective June 20, 2022.*

1350-03-.03 USER ACCESS CONTROLS FOR ALL INTERACTIVE SPORTS GAMING PERSONNEL.

(1) A system administrator shall establish user accounts for all new employees responsible for or with duties relating to Interactive Sports Gaming in the State of Tennessee. Provisioning for user accounts consists of assigning application functions matching the employee's job responsibilities, unless otherwise authorized by management personnel, to ensure adequate separation of duties.

(2) The access provisioning process must be documented. Documentation must evidence authorization by the appropriate management personnel, original user access, and each subsequent change to the user account. Documentation must be maintained and made available upon request to the Council.

(3) A Sports Gaming System must store "User Access Listing" information and contain at a minimum:

(a) Employee name and title or position;

(b) User login name;

(c) Full list and description of application functions that each group/user account may execute;

(d) Date and time account created;

(e) Date and time of last login;

(f) Date of last password change;

(Rule 1350-03-.03, continued)

(g) Date and time account disabled/deactivated; and

(h) Group membership of user account, if applicable.

(4) "User Access Listing" information for the Sports Gaming System is to be retained for the most recent five (5) years. The information may be archived electronically if the listing is written to unalterable media (secured to preclude alteration). The list of users and user access for a Sports Gaming System must be available in electronic format that can be analyzed by analytical tools (e.g., spreadsheet or database) that may be employed by the Council.

(5) When multiple user accounts are used for one employee within a single application, only one user account may be active (enabled) at a time if the concurrent use of the multiple accounts by the employee could create a segregation of duties deficiency. Additionally, the user account must have a unique prefix/suffix to easily identify the users with multiple user accounts within one application.

(6) The system administrator must be notified Immediately when an employee, including one who has a user account with remote access capability, is known to be no longer employed (e.g., voluntary or involuntary termination of employment). Hostile terminations require immediate notification to the system administrator who must promptly disable/remove access rights to the system(s). Upon notification, the system administrator must change the status of the employee's user account from active to inactive (disabled) status.

The period of time for notification of the system administrator is to be set such that it is unlikely that the terminated employee would gain access, remote or otherwise, within the notification period.

(7) The "User Access Listing" information must be reviewed at least quarterly by personnel independent of the authorization and user provisioning processes. The reviewer must maintain adequate evidence to support the review process, which includes the selected user accounts reviewed, documentation of the results of the review, and e-mails or signatures and dates indicating the individual(s) performing the review and when the user access listing was reviewed. For each of the randomly selected users, confirm that:

(a) The assigned system functions are being used as authorized (i.e., system functions are appropriate for user's job position);

(b) The assigned functions provide an adequate segregation of duties;

(c) Terminated employees' user accounts have been changed to inactive (disabled) status;

(d) Passwords have been changed within the last 60-90 days; and

(e) There are no inappropriate assigned functions for group membership, if applicable.

Authority: *T.C.A. §§ 4-49-106, 4-49-110, 4-49-115, and 4-49-125.* ***Administrative History:*** *Emergency rules filed December 22, 2021 to become effective January 1, 2022; effective through June 30, 2022. New rules filed March 22, 2022; effective June 20, 2022.*

1350-03-.04 SEGREGATION OF DUTIES.

(1) Each Licensee shall maintain an organizational structure that meets the following minimum criteria designed to preserve the integrity of the Interactive Sports Gaming operation:

(Rule 1350-03-.04, continued)

(a) A system of personnel and chain of command which permits management and supervisory personnel to be held accountable for actions or omissions within their area of responsibility;

(b) The segregation of incompatible functions so that no employee is in a position either to commit an error or perpetrate a fraud or to conceal an error or fraud in the normal course of his or her duties;

(c) Primary and secondary supervisory positions which permit the authorization or supervision of necessary transactions at all relevant times; and

(d) Areas of responsibility that are not so extensive as to be impractical for one individual to monitor.

(2) In addition to satisfying the above requirements, each Licensee's organizational structure shall include, at a minimum, the following functions, responsibilities, and supervisory roles:

(a) Accounting.

1. Each Licensee shall have one or more individuals responsible for and dedicated to verifying financial transactions, and reviewing and controlling accounting forms and data. This function, which is sometimes referred to as "income or revenue audit," shall be independent of the transactions under review.

2. Key Personnel serving as accounting officer, or equivalent, shall supervise the accounting functions, responsibilities, and supervisory roles as provided for in this section.

(b) Interactive Sports Gaming.

1. Each Licensee shall have Interactive Sports Gaming functions, responsibilities, and supervisory roles for Interactive Sports Gaming, which shall be responsible for the conduct of the Interactive Sports Gaming in accordance with the Rules.

2. Interactive Sports Gaming shall be supervised by a management-level employee who ensures that there is sufficient supervision, knowledge, and training to provide for the proper and fair conduct of sports gaming.

3. Key Personnel shall supervise the Interactive Sports Wagering functions, responsibilities, and supervisory roles as provided for in this section.

(c) Internal Audit.

1. Each Licensee shall maintain an Internal Audit function for Interactive Sports Gaming either through an employee serving as internal auditor with sufficient background and experience to fulfill the role, through the use of company Internal Audit, or through outsourcing of this function. The Internal Audit function shall be responsible for, without limitation, the following:

(i) Reviewing and appraising the adequacy of internal controls;

(ii) Ensuring compliance with internal controls through observations, interviews and review of accounting documentation; and

(iii) Reporting instances of non-compliance with the system of internal controls.

(Rule 1350-03-.04, continued)

2. Reporting of any material weaknesses in the system of internal controls.

3. Recommending improvements in the system of internal controls.

4. If maintained in-house, the Internal Audit function shall be supervised by Key Personnel serving as accounting officer, or equivalent.

5. The Internal Audit function shall maintain its independence through an organizational reporting line that is outside the management of the sports gaming operation. The supervisor of the Internal Audit function shall have authority to access and report to any Person or group independent of the business, such as to a non-executive independent director, compliance committee member, or independent audit committee.

6. Reports documenting audits performed shall be maintained for a minimum of five years and shall be made available to the Council upon request.

7. All material exceptions resulting from Internal Audit work shall be investigated and resolved with the results of such being documented and retained for a minimum of five years.

8. Internal Audit findings shall be reported to management and any instances of non-compliance shall be reported Immediately to the Council.

9. Management shall be required to respond to Internal Audit findings stating corrective measures to be taken to avoid recurrence of the audit exception. A report on corrective measures to be taken shall be sent to the Council simultaneously with or within ten (10) days of the Internal Audit non-compliance report.

(d) Management Information Systems (MIS).

1. Each Licensee shall maintain an MIS function, which shall be responsible for the operation and integrity of the Sports Gaming System and the quality, reliability, and accuracy of all computer systems used in the operation.

2. The MIS function shall be responsible for, without limitation, the specification of appropriate computer software, hardware, and procedures for security, physical integrity, business continuity, and maintenance of:

(i) Access codes and other data-related security controls used to ensure appropriately limited access to computers and the system-wide reliability of data;

(ii) Computer tapes, disks, or other electronic storage media containing data relevant to sports wagering operations;

(iii) Computer hardware, communications equipment and software used in the conduct of sports gaming operations; and

(iv) Adequate segregation of duties exists among developers, testing personnel, administrators, personnel who may promote changes into production, personnel who may access frozen code, etc.

3. Key Personnel holding the position of an administrative officer, or equivalent, shall supervise the MIS function.

(Rule 1350-03-.04, continued)

4. All incidents related to information systems security, which may compromise the confidentiality, integrity, or availability of the Sports Gaming System, or involving Player Personally Identifiable Information (PII) shall be reported to the Council Immediately.

(e) Compliance

1. Each Licensee shall maintain a Compliance function, which shall be responsible for, without limitation, the following:

(i) Due diligence and regulating reporting requirements;

(ii) Serving as contact with the Council on regulatory matters;

(iii) Monitoring self-exclusion program;

(iv) Player complaints;

(v) Investigating Unusual and Suspicious Wagering Activity; and

(vi) AML monitoring and reporting pursuant to federal law.

2. Key Personnel serving in the role of a compliance officer, or equivalent, shall supervise the Compliance function.

Authority: *T.C.A. §§ 4-49-106, 4-49-110, 4-49-115, and 4-49-125.* ***Administrative History:*** *Emergency rules filed December 22, 2021 to become effective January 1, 2022; effective through June 30, 2022. New rules filed March 22, 2022; effective June 20, 2022.*

1350-03-.05 RISK MANAGEMENT PROCEDURES.

Each Sports Gaming System submitted to the Council for approval shall contain a description of its risk management framework.

Authority: *T.C.A. §§ 4-49-106, 4-49-110, 4-49-115, and 4-49-125.* ***Administrative History:*** *Emergency rules filed December 22, 2021 to become effective January 1, 2022; effective through June 30, 2022. New rules filed March 22, 2022; effective June 20, 2022.*

1350-03-.06 IDENTIFYING AND REPORTING FRAUD AND UNUSUAL AND SUSPICIOUS ACTIVITIES.

A Licensee shall have Integrity Monitoring System Procedures in place to identify Unusual and Suspicious Wagering Activity and report such activity in accordance to procedures approved by the Council.

(1) The Licensee's Integrity Monitoring System Procedures shall include a requirement that the Licensee submit all reports of Unusual and Suspicious activity to the Council and shall provide for sharing information with other Licensees, through an Independent Integrity Monitoring Association, as necessary.

(2) If a Licensee finds that previously reported Unusual Wagering Activity rises to the level of Suspicious Wagering Activity or if an activity constitutes Suspicious Wagering Activity, it shall Immediately Notify the Council.

(3) The monitoring and reporting requirements for Unusual and Suspicious activity, include, at a minimum:

(Rule 1350-03-.06, continued)

(a) Attempts to violate or evade any federal, state, or local law or regulations pertaining to Interactive Sports Gaming in any jurisdictions;

(b) Violations or attempted violations of federal or state Anti-Money Laundering (AML) laws;

(c) Unusual or suspicious behavior or patterns of Wagers by Player as determined by the Licensee;

(d) Unusual geographical concentration betting;

(e) Wagers that have been placed online or through a mobile device using different accounts but having the same IP address;

(f) Unusual and abnormal proportion of Bets against the favorite or for the underdog; or

(g) Unusual volumes of betting relative to the norm.

(4) A Licensee must also submit an annual report to the Council which details its integrity monitoring services and activities and summarizes all Unusual Wagering Activity or Suspicious Wagering Activity notifications issued during the year.

(5) If the Council receives an Unusual or Suspicious Wagering Activity report from a Licensee, the information shall be deemed confidential and shall not be revealed in whole or in part, except upon lawful order of a court of competent jurisdiction or upon notice or referral of a matter for further investigation to any law enforcement agency, regulatory or government agency, or sports governing body within the sole and absolute discretion of the Council.

(6) Upon request by the Council or the Executive Director, a Licensee shall provide remote, read-only access and the necessary hardware for the Council to evaluate or monitor the Sports Gaming System.

Authority: *T.C.A. §§ 4-49-106, 4-49-110, 4-49-115, 4-49-122, and 4-49-125.* ***Administrative History:*** *Emergency rules filed December 22, 2021 to become effective January 1, 2022; effective through June 30, 2022. New rules filed March 22, 2022; effective June 20, 2022.*

1350-03-.07 PREVENTION OF INTERACTIVE SPORTS GAMING BY INELIGIBLE BETTORS.

Each Licensee shall submit to the Council its methodology for preventing a Bettor who is ineligible due to his/her inclusion in one or more classes of ineligible Bettors as enumerated in the Sports Gaming Act, § 4-49-112 from placing a Wager on Sporting Events or collecting winnings from Interactive Sports Gaming.

Authority: *T.C.A. §§ 4-49-106, 4-49-110, 4-49-112, 4-49-115, and 4-49-125.* ***Administrative History:*** *Emergency rules filed December 22, 2021 to become effective January 1, 2022; effective through June 30, 2022. New rules filed March 22, 2022; effective June 20, 2022.*

1350-03-.08 AML AND REGULATORY COMPLIANCE STANDARDS.

(1) Each Licensee shall submit to the Council for approval a description of its AML and regulatory compliance programs, policies, and procedures.

(2) Each Licensee shall notify the Council Immediately upon discovery and knowledge of any violation or non-compliance with the AML compliance program, policies, and procedures; AML laws or regulations; any regulatory compliance program, policies, and procedures; or any law or regulation governing the Licensee in any jurisdiction, including the State of Tennessee.

(Rule 1350-03-.08, continued)

Authority: *T.C.A. §§ 4-49-106, 4-49-110, 4-49-115, and 4-49-125.* ***Administrative History:*** *Emergency rules filed December 22, 2021 to become effective January 1, 2022; effective through June 30, 2022. New rules filed March 22, 2022; effective June 20, 2022.*

1350-03-.09 TYPES OF WAGERS AVAILABLE.

(1) Each Licensee shall only offer Wagers on Sporting Events approved by the Council, a list of which shall be posted on the Council's website. The Council shall notify Licensees when a Sporting Event is no longer included on the list of approved Sporting Events upon which Wagers may be placed or accepted.

(2) Any entity may petition the Council for approval of a new Sporting Event upon which Wagers may be placed or accepted.

(a) A petition for approval of a proposed new Sporting Event must be in writing and submitted a minimum of 72 hours prior to being offered.

(b) A proposed new Sporting Event may be a variation of an authorized sports wagering Event, a composite of authorized Sporting Events, or any other Sporting Event compatible with the public interest.

(c) A petition for a proposed new Sporting Event shall be in writing, signed by the petitioner, and shall include the following information:

1. The name of the petitioner;

2. Whether the new Sporting Event is a variation of an authorized Sporting Event, a composite of authorized Sporting Events, or any other Sporting Event compatible with the public interest;

3. A complete and detailed description of the new Sporting Event for which approval is sought;

4. Evidence of governing body rules and regulations or independent integrity monitoring of the new Sporting Event; and

5. Any other pertinent information or material requested by the Council.

(d) No Wagers may be accepted on a proposed Sporting Event until it has been approved by the Council.

Authority: *T.C.A. §§ 4-49-106, 4-49-110, 4-49-115, 4-49-122, and 4-49-125.* ***Administrative History:*** *Emergency rules filed December 22, 2021 to become effective January 1, 2022; effective through June 30, 2022. New rules filed March 22, 2022; effective June 20, 2022.*

1350-03-.10 THIRD-PARTY SYSTEMS.

(1) The Licensee shall have policies and procedures for managing third parties who provide information system services, hardware, and/or software or interact with the Sports Gaming System. Licensees are responsible for monitoring their adherence to relevant security requirements, including:

(a) Agreements with third-party service providers involving accessing, processing, communicating, or managing the system and/or its components, or adding products or services to the system and/or its components shall cover all relevant security requirements.

(Rule 1350-03-.10, continued)

(b) The services, reports, and records provided by the third-party service providers shall be monitored and reviewed annually.

(c) Changes to the provision of third-party service providers, including maintaining and improving existing security policies, procedures, and controls, shall be managed, taking account of the criticality of systems and processes involved and re-assessment of risks.

(d) The access rights of third-party service providers to the system and/or its components shall be removed upon termination of their contract or agreement or adjusted upon change.

(e) Verification that third-party service providers are registered as a Vendor in accordance with the Rules as may be required.

(2) Third parties who provide information system services and/or software must comply with the requirements set forth in Sections 1350-03-.12 and 1350-03-.13.

Authority: *T.C.A. §§ 4-49-106, 4-49-110, 4-49-115, and 4-49-125.* ***Administrative History:*** *Emergency rules filed December 22, 2021 to become effective January 1, 2022; effective through June 30, 2022. New rules filed March 22, 2022; effective June 20, 2022.*

1350-03-.11 PROHIBITION ON WAGERS AND PAYOUTS TO MINORS.

(1) Licensees shall not permit Sports Gaming Accounts to be established, deposits to be made by, or Wagers to be placed by Minors. Each Licensee shall maintain a system through which it verifies the age and identity of the Bettor and verifies that Wagers are not made by Minors. This system shall be approved by the Council through the Sports Gaming Operating System Assessment.

(2) Licensees shall establish procedures to reasonably ensure a Bettor who is a Minor is prohibited from participating in Interactive Sports Gaming and such procedures are delineated within the Licensee's written system of internal controls. These procedures, at a minimum, shall include:

(a) Verification of the full identify of the Bettor prior to the Bettor being allowed to make a deposit into his/her Sports Gaming Account or making a Wager on a Sporting Event; and

(b) Verification of the Bettor's age through a recognized national database or service (or other commercially reasonably standard for age verification) using at a minimum the Player's full name, date of birth, and last four (4) digits of the Bettor's social security number or taxpayer identification.

(3) Licensees shall provide the Council information about its procedures or methodology for verifying the age of a Bettor. Licensee shall notify the Council of any changes to its procedures or in the event there is a change of a Vendor, as applicable, that provides age verification services to the Licensee.

(4) Licensees shall prohibit any Minor from collecting payouts or winnings from Interactive Sports Gaming.

Authority: *T.C.A. §§ 4-49-106, 4-49-110, 4-49-111, 4-49-115, and 4-49-125.* ***Administrative History:*** *Emergency rules filed December 22, 2021 to become effective January 1, 2022; effective through June 30, 2022. New rules filed March 22, 2022; effective June 20, 2022.*

1350-03-.12 INFORMATION SYSTEM MINIMUM CONTROLS.

(1) Licensees shall verify Sports Gaming Systems daily to ensure the date and time is properly displayed and registered for Wagers made pursuant to Sports Gaming Accounts. Licensees shall Immediately Report any discrepancies to the Council.

(2) Licensee shall implement an Integrity Monitoring System utilizing software to identify irregularities in volume or odds and swings that could signal Unusual or Suspicious Wagering Activities that should require further investigation and shall Immediately Report such findings to the Council.

(3) Sports Gaming Systems shall be designed to only allow Wagers to be created using an authorized Sports Gaming Account.

(4) Sports Gaming Systems shall contain a mechanism to prevent the creation of a Wager before or after the official Wager timeframe (i.e., prior to posting of the Wager and subsequent to the outcome of a Sporting Event or cutoff).

(5) Sports Gaming Systems shall be incapable of voiding a Wager subsequent to the outcome of a Sporting Event or cutoff.

(6) Sports Gaming Systems shall automatically authorize payment of winning Wagers and update a Player's Sports Gaming Account.

(7) Sports Gaming Systems shall be incapable of authorizing payment on a Wager that has been previously paid or voided.

(8) Sports Gaming Systems shall be designed to prevent an individual, group of individuals or entity from tampering with or interfering with the operation of Interactive Sports Gaming or Sports Gaming Systems.

(9) Sports Gaming Systems shall be configured to terminate a Player's session, and/or require re-authentication, after a prescribed period of inactivity by the Player not to exceed thirty (30) minutes.

(10) Sports Gaming Systems shall be configured to lock Player Sports Gaming Accounts after three (3) failed login attempts. If the Licensee allows accounts to unlock automatically after a prescribed amount of time has elapsed, Multi-Source Authentication shall be required on the next login.

(11) Sports Gaming Systems shall be designed to ensure the integrity and confidentiality of all communications and ensure the proper identification of the sender and receiver of all communications. If communications are performed across a public or third-party network, the system shall either encrypt the data packets or utilize a secure communications protocol to ensure the integrity and confidentiality of the transmission.

(12) Confidential and/or sensitive electronic data shall be encrypted while both at rest or in transit using the current standards and methodologies set forth in Special Bulletins issued by the National Institute of Standards and Technology (NIST). Confidential and/or sensitive electronic data may include, but is not limited to, Sports Gaming System and Player passwords, Player PII, and Player banking information.

(13) User authentication to the Sports Gaming Systems and other system components shall be configured consistent with the current standards and methodologies set forth in Special Bulletins issued by the NIST.

(Rule 1350-03-.12, continued)

(14) Sports Gaming Systems shall monitor for and Immediately Report to the Licensee and the Council any malfunction or security incident that adversely affects the integrity of critical data or system functionality.

(15) A system event log or series of reports/logs for operating systems (including the database layer and network layer) and applications must be configured to track at least the following events:

(a) Failed login attempts;

(b) Changes to live data files occurring outside of normal program and operating system execution;

(c) Changes to operating system, database, network, and application policies and parameters;

(d) Audit trail of information changed by administrator accounts;

(e) Changes to date/time on master time server;

(f) Significant periods of unavailability of the Sports Gaming System or any critical component of the Sports Gaming System; and

(g) Other significant events.

(16) Sports Gaming Systems shall record and generate daily reports that may be accessed and reviewed by the Council upon request on the following:

(a) Wagers exceeding $10,000;

(b) Futures Wagers;

(c) Sports Gaming Account activity, including Sports Gaming Account number, transaction, and transaction amount. The report must include deposit amounts, withdrawal amounts, winnings, and Wagers made; and

(d) Changes in odds, Wager cutoff times, Event data, or Sporting Event results.

(17) Sports Gaming Account management shall be configured in a manner to ensure the confidentiality and integrity of the Player PII and to protect the Sports Gaming Account from unauthorized use. The following controls surrounding Sports Gaming Accounts must be present at a minimum:

(a) Once a Sports Gaming Account is created, a secure personal identification for the Player authorized to use the Sports Gaming Account shall be established that is reasonably designed to prevent the unauthorized access to, or use of, the Sports Gaming Account by any individual other than the Player for whom the Sports Gaming Account is established;

(b) Controls shall be in place to ensure the strength of Player’s passwords;

(c) A Player shall have only one (1) Sports Gaming Account per Licensee;

(d) Player’s Sports Gaming Account shall be Immediately suspended, and Player’s identification shall be Immediately re-verified upon reasonable suspicion that the Player’s identification has been compromised;

(Rule 1350-03-.12, continued)

(e) Player's Sports Gaming Account shall be disabled after three failed log-in attempts and require Multi-Source Authentication to recover or reset a password or username;

(f) Multi-Source Authentication shall be required before allowing a Player to reset the Sports Gaming Account password, access/update Player PII, transfer funds, unlock the Sports Gaming Account, or to remove a Player from the Licensee's self-exclusion list;

(g) Players shall be allowed to manage their profiles at all times when logged in regardless of their geographical location; and

(h) A mechanism shall be in place to suspend a Player's Sports Gaming Account in the event that there is suspicion that the Sports Gaming Account has been compromised or used to commit fraud or other illegal activity.

(18) Licensees shall have policies and procedures for all changes to the Sports Gaming System and its related components. Documentation must be created and maintained for all changes to the production environment of the Sports Gaming System and its related components.

(19) The Licensee shall have a documented process for performing and restoring Sports Gaming System back-ups. All backup media must be stored at a secure location offsite. Periodic testing of backup media must be performed to ensure that the Sports Gaming System can be restored in the event of a failure.

(20) The integrity of all geolocation systems used by the Licensee shall be reviewed regularly to ensure it detects and mitigates existing and emerging location fraud risks. Evidence that the geolocation system in use is updated to the latest version shall be provided to the Council at least every one hundred and eighty (180) days.

(21) Interactive Sports Gaming may only be conducted over the Internet or through the use of Mobile applications or other digital platforms. The internal controls for the Sports Gaming Systems shall apply to all websites and applications used to provide this functionality.

(22) Additional system specifications and Sports Gaming Systems logging requirements may be specified by the Council through the issuance of technical bulletins in the case of exigent circumstances.

(23) Each Licensee shall Immediately Report to the Council any known violations or incidents of non-compliance with any part of this chapter.

Authority: *T.C.A. §§ 4-49-106, 4-49-110, 4-49-115, 4-49-122, and 4-49-125.* ***Administrative History:*** *Emergency rules filed December 22, 2021 to become effective January 1, 2022; effective through June 30, 2022. New rules filed March 22, 2022; effective June 20, 2022.*

1350-03-.13 INFORMATION SYSTEM AUDIT REQUIREMENTS.

A Sports Gaming System shall, at least once every twenty-four (24) hours, perform a self-authentication process on all software used to offer, record, and process Wagers to ensure there have been no unauthorized modifications. In the event of an authentication failure, at a minimum, the Sports Gaming System shall Immediately Notify the Licensees' Information Systems Officer, or equivalent, and the Council within twenty-four (24) hours. The results of all self-authentication attempts shall be recorded by the system and maintained for a period of not less than ninety (90) days.

Authority: *T.C.A. §§ 4-49-106, 4-49-110, 4-49-115, and 4-49-125.* ***Administrative History:*** *Emergency rules filed December 22, 2021 to become effective January 1, 2022; effective through June 30, 2022. New rules filed March 22, 2022; effective June 20, 2022.*