Attachment B

Internet Sports Betting ICS Requirements

**Items at a Minimum That Must be Included in Internet Sports Betting ICS:**

**Section 1: Platform Operation**

1. Procedures for responding to a failure of the sports betting platform (i.e. game, system, communications, or platform malfunction), including procedures for restoring sports betting operations. Incident report for each significant platform failure must be filed with the board and contain the date, time, and reason for the failure along with the date and time the system was restored.
2. Detail the location of the sports betting servers, including any third-party remote location servers, and what controls will be in place to ensure security of the sports betting servers.
3. Technical security standards (controls), which must address all of the following:
	1. Applicability and Scope.
		1. The technical security standards must apply, at a minimum, to all the following critical components of the internet sports betting platform:
			1. Components which record, store, process, share, transmit or retrieve sensitive information (e.g., validation numbers, personal identification number (PIN), individual and authorized participant data).
			2. Components which store results or the current state of an authorized participant’s internet sports betting wager.
			3. Points of entry to and exit from the components provided for in subsection (a-c) and other systems which are able to communicate directly with core critical internet sports betting platform components.
			4. Communication networks which transmit sensitive information involving sports betting under the act.
	2. General Requirements.
		1. The technical security standards (controls) must:
			1. Include a provision requiring review when changes occur to the internet sports betting platform.
			2. Be approved by the sports betting operator’s or internet sports betting platform provider’s senior management.
			3. Be communicated to all affected employees and relevant external parties.
			4. Undergo review at planned intervals.
			5. Delineate the responsibilities of the sports betting operator’s staff, the internet sports betting platform provider’s staff, and the staff of any third parties for the operation, service, and maintenance of the internet sports betting platform and/or its components.
			6. Meet or exceed the standards prescribed in Gaming Laboratories International, LLC Standard GLI-33: Standards for Event Wagering Systems, version 1.1, released May 14, 2019.
	3. Internet Sports Betting Platform Operations and Security.
		1. Internet Sports Betting Platform Operations and Security. The sports betting operator or internet sports betting platform provider must adopt, implement, and maintain procedures for, at a minimum, the following:
			1. Monitoring the critical components and the transmission of data of the entire internet sports betting platform.
			2. Maintenance of all aspects of security of the internet sports betting platform to ensure secure and reliable communications.
			3. Defining, monitoring, documenting, reporting, investigating, responding to, and resolving security incidents.
			4. Monitoring and adjusting resource consumption and maintaining a log of the internet sports betting platform performance.
			5. Investigating, documenting, and resolving malfunctions.
		2. Physical Location of Servers and Security. The internet sports betting platform must be housed in secure locations. Sports betting operators and their internet sports betting platform providers must provide the board with information on the location of all internet sports betting platform servers. The secure locations must have sufficient protection from unauthorized access and physical and environmental hazards and be equipped with surveillance and security systems that meet or exceed industry standards.
		3. Internet Sports Betting Platform Logical Access Controls. The internet sports betting platform must be logically secured against unauthorized access.
		4. Internet Sports Betting Platform User Authorization. The internet sports betting platform must be subject to user authorization requirements as required by the board.
		5. Server Programming. The internet sports betting platform must be sufficiently secure to prevent any user-initiated programming capabilities on the server that may result in unauthorized modifications to the database.
		6. Verification Procedures. Procedures must be in place for verifying on demand that the critical control program components of the internet sports betting platform in the production environment are identical to those approved by the board.
		7. Electronic Document Retention System. The sports betting operator or internet sports betting platform provider must establish procedures that ensure that all reports required under the Lawful Sports Betting Act (act) and related rules are stored in an electronic document retention system.
		8. Asset Management. All assets that house, process, or communicate sensitive information, including those comprising the operating environment of the internet sports betting platform and/or its components, must be accounted for and have a nominated owner or designated management official that is responsible for each asset.
	4. Backup and Recovery.
		1. Data Security. The internet sports betting platform must provide a logical means for securing individual and authorized participant data and wagering data, including accounting, reporting, significant event, or other sensitive information, against alteration, tampering, or unauthorized access.
		2. Data Alteration. The alteration of any accounting, reporting, or significant event data relating to sports betting under the act will not be permitted without supervised access controls. In the event any data is changed, all information required by the board must be documented or logged.
		3. Backup Frequency. Backup scheme implementation relating to information involving sports betting under the act must occur at least once every day or as otherwise specified by the board.
		4. Storage Medium Backup. Audit logs, internet sports betting platform databases, and any other pertinent individual and authorized participant data and wagering data must be stored using reasonable protection methods. The internet sports betting platform must be designed to protect the integrity of this data in the event of a failure. Redundant copies of this data must be kept on the internet sports betting platform with open support for backups and restoration, so that no single failure of any portion of the internet sports betting platform would cause the loss or corruption of such data.
		5. Internet Sports Betting Platform Failure. The internet sports betting platform must have sufficient redundancy and modularity so that if any single component or part of a component fails, the functions of the internet sports betting platform and the process of auditing those functions can continue with no critical data loss. When two or more components are linked, the process of all internet sports betting operations between the components must not be adversely affected by restart or recovery of either component and upon restart or recovery, the components must immediately synchronize the status of all transactions, data, and configurations with one another.
		6. Accounting and Master Resets. The sports betting operator or internet sports betting platform provider must be able to identify and properly handle the situation where a master reset has occurred on any component which affects sports betting under the act.
		7. Recovery Requirements. In the event of a catastrophic failure when the internet sports betting platform cannot be restarted in any other way, it must be possible to restore the internet sports betting platform from the last backup point and fully recover. The contents of that backup must contain critical information as required by the board.
		8. Uninterrupted Power Supply (UPS) Support. All internet sports betting platform components must be provided with adequate primary power. Where the server is a stand-alone application, it must have a UPS connected and must have sufficient capacity to permit a methodical shut-down that retains all individual and authorized participant data and wagering data during a power loss. It is acceptable that the internet sports betting platform may be a component of a network that is supported by a network-wide UPS provided that the server is included as a device protected by the UPS. There must be a surge protection system in use if not incorporated into the UPS itself.
		9. Business Continuity and Disaster Recovery Plan. A business continuity and disaster recovery plan must be in place to recover internet sports betting operations conducted under the act if the internet sports betting platform’s production environment is rendered inoperable.
	5. Communications.
		1. Connectivity. Only authorized wagering devices are permitted to establish communications between any internet sports betting platform components.
		2. Communication Protocol. Each component of the internet sports betting platform must function as indicated by a documented secure communication protocol.
		3. Communication Over Internet/Public Network. Communications between internet sports betting platform components must be secure. Individual and authorized participant data, sensitive information, internet wagers, results, financial information, and individual and authorized participant transaction information related to sports betting conducted under the act must always be encrypted and protected from incomplete transmissions, misrouting, unauthorized message modification, disclosure, duplication, or replay.
		4. Wireless Local Area Network (WLAN) Communications. The use of WLAN communications must adhere to applicable requirements specified for wireless devices and are subject to approval by the board.
		5. Network Security Management. Networks must be logically separated to ensure that there is no network traffic on a network link which cannot be serviced by hosts on that link.
	6. Third Party Service Providers.
		1. Third-Party Service Communications. Where communications related to sports betting conducted under the act are implemented with third-party service providers, the internet sports betting platform must securely communicate with all third-party service providers utilizing encryption and strong authentication, ensure that all login events are recorded to an audit file, and ensure that all communications do not interfere or degrade normal internet sports betting platform functions.
		2. Third-Party Services. The roles and responsibilities of each third-party service provider engaged by the sports betting operator or internet sports betting platform provider must be defined and documented in a manner approved by the board. The sports betting operator or internet sports betting platform provider must have policies and procedures in place for managing third-party service providers and monitoring their adherence to relevant security requirements.
	7. Technical Controls.
		1. Domain Name Service (DNS) Requirements. A sports betting operator or internet sports betting platform provider must establish requirements that apply to servers used to resolve DNS queries used in association with the internet sports betting platform.
		2. Cryptographic Controls. A sports betting operator or internet sports betting platform provider must establish and implement a policy for the use of cryptographic controls that ensures the protection of information.
		3. Encryption Key Management. The management of encryption keys must follow defined processes established by the sports betting operator or internet sports betting platform provider and approved by the board.
	8. Remote Access and Firewalls.
		1. Remote Access Security. Remote access, if approved by the board, must be performed via a secured method, must have the option to be disabled, may accept only the remote connections permissible by the firewall application and internet sports betting platform settings, and must be limited to only the application functions necessary for users to perform their job duties.
		2. Remote Access and Guest Accounts Procedures. Remote access and guest accounts procedures must be established that ensure that remote access is strictly controlled.
		3. Remote Access Activity Log. The remote access application must maintain an activity log which updates automatically and records and maintains all remote access information.
		4. Firewalls. All communications, including remote access, must pass through at least one approved application-level firewall. This includes connections to and from any non-internet sports betting platform hosts used by the sports betting operator or internet sports betting platform provider.
		5. Firewall Audit Logs. The firewall application must maintain an audit log and must disable all communications and generate an error if the audit log becomes full. The audit log must contain, at a minimum, all the following information:
			1. All changes to configuration of the firewall.
			2. All successful and unsuccessful connection attempts through the firewall.
			3. The source and destination IP Addresses, Port Numbers, Protocols, and where possible, MAC Addresses.
		6. Firewall Rules Review. The firewall rules must be periodically reviewed by the sports betting operator or internet sports betting platform provider to verify the operating condition of the firewall and the effectiveness of its security configuration and rule sets and must be performed on all the perimeter firewalls and the internal firewalls.
	9. Change Management.
		1. Program Change Control Procedures. Program change control procedures must ensure that only authorized versions of programs are implemented on the production environment.
		2. Software Development Life Cycle. The acquisition and development of new software must follow defined processes established by the sports betting operator or internet sports betting platform provider and subject to review by the board.
		3. Patches. All patches should be tested, as applicable, in a development and test environment configured to match the target production environment before being deployed into production. Permitted exceptions, related procedures, and controls must be fully addressed.
	10. Periodic Security Testing.
		1. Technical Security Testing. Periodic technical security tests on the production environment must be performed quarterly or as required by the board to guarantee that no vulnerabilities putting at risk the security and operation of the internet sports betting platform exist.
		2. Vulnerability Assessment. The sports betting operator or the internet sports betting platform provider must conduct vulnerability assessments. The purpose of the vulnerability assessment is to identify vulnerabilities, which could be later exploited during penetration testing by making basic queries relating to services running on the internet sports betting platform concerned.
		3. Penetration Testing. The sports betting operator or the internet sports betting platform provider must conduct penetration testing. The purpose of the penetration testing is to exploit any weaknesses uncovered during the vulnerability assessment on any publicly exposed applications or internet sports betting platform hosting applications processing, transmitting, and/or storing sensitive information.
		4. Information Security Management System (ISMS) Audit. An audit of the ISMS will be periodically conducted, including all the locations where sensitive information is accessed, processed, transmitted, and/or stored. The ISMS will be reviewed against common information security principles in relation to confidentiality, integrity, and availability.
		5. Cloud Service Audit. A sports betting operator and its internet sports betting platform provider that utilizes a cloud service provider (CSP), if approved by the board, to store, transmit, or process sensitive information must undergo a specific audit as required by the board. The CSP will be reviewed against common information security principles in relation to the provision and use of cloud services, such as ISO/IEC 27017 and ISO/IEC 27018, or equivalent.
4. Procedures addressing the internet sports betting platform’s communication standards.
5. Procedures addressing the internet sports betting platform’s data logging standards.
6. Procedures to review the completeness, accuracy, reliability, timeliness, and availability of any data feeds used to offer or settle internet sports betting wagers.
7. Define and provide procedures for “obvious error,” since a sports betting operator or internet sports betting platform provider may, in its discretion, cancel an accepted internet sports betting wager for obvious error.
8. Description of all integrated third-party platforms.
9. Procedures for geofencing system verifying each authorized participant’s physical location is located within the permitted boundary when placing a wager.
10. User access controls for all sports betting personnel.
11. Segregation of duties.
12. Automated and manual risk management procedures.
13. Procedures and security standards as to receipt, handling, and storage of sports betting equipment.

**Section 2: Acceptance of Wagers, Title 31, and Integrity Monitoring/Suspicious Behavior**

1. Description of anti-money laundering compliance standards.
2. Description of process for accepting wagers and issuing payouts, plus any additional controls for accepting wagers and issuing payouts in excess of $10,000.
3. Procedures for identifying and reporting fraud and suspicious conduct including identifying unusual wagering activity and reporting such activity to an independent integrity monitoring provider.
4. Description of process for accepting multiple wagers from one authorized participant in a 24-hour cycle, including process to identify authorize participant structuring of wagers to circumvent recording and reporting requirements.
5. Process for submitting or receiving approval for all event categories and wager types available.
6. Procedures for issuance and acceptance of promotional funds for internet sports betting.
7. Description of the process for line setting and line moving.
8. Procedures and appropriate measures implemented to deter, detect and, to the extent possible, to prevent cheating, including collusion, and use of cheating devices, including the use of software programs that make bets according to algorithms.
9. Automated and manual risk management procedures.

**Section 3: Accounting**

1. Procedures and security for the calculation and recording of gross sports betting receipts, adjusted gross sports betting receipts and winnings.
2. Policies and procedures in connection with the internal audit function of its sports betting operations.
3. Procedure for the recording of and reconciliation of internet sports betting transactions.
4. Segregation of duties.

**Section 4: Authorized Participants**

1. Procedures for identifying and restricting prohibited persons.
2. Description of process to close out dormant accounts.
3. Description of process for voiding or cancelling wagers and refunding the authorized participant.
4. Procedures for making adjustments to an internet sports betting account (including adjustments for $500 or under must be periodically reviewed by supervisory personnel and anything over $500 must be authorized by supervisory personnel), providing a method for an authorized participant to close out an account and how an authorized participant will be refunded after the closure of an account or how funds will be escheated.
5. Methods for securely issuing, modifying, and resetting an authorized participants account password, Personal Identification Number (PIN), or other approved security feature, where applicable. Any method must include notification to the authorized participant following any modification via electronic or regular mail, text message, or other manner approved by the board. Such methods must include, at a minimum, one of the following:
	1. Proof of identity, if in person.
	2. The correct response to two or more challenge questions.
	3. Strong authentication.
6. Procedures for terminating an internet sports betting account and the return of any funds remaining in the internet sports betting account to the authorized participant or confiscation of funds.
7. Procedures to terminate all accounts of any individual who establishes or seeks to establish multiple active internet sports betting accounts, whether directly or by use of another individual as a proxy.
8. Procedures for receiving, investigating, and responding to all authorized participant complaints.
9. Procedures for registration of authorized participants and establishing internet sports betting accounts, including a procedure for authenticating the age, identity and physical address of an applicant for an internet sports betting account and whether the applicant is prohibited from establishing or maintaining an account under applicable laws or regulations.
10. Procedures for handling authorized participants or other individuals discovered to be using internet sports betting accounts in a fraudulent manner, including the following:
	1. The maintenance of information about any authorized participant’s activity or other individual’s activity, such that if fraudulent activity is detected, the sports betting operator or internet sports betting platform provider and the board have all of the necessary information to take appropriate action.
	2. The suspension of any internet sports betting account discovered to be providing fraudulent access to prohibited persons.
	3. The treatment of deposits, internet sports wagers, and wins associated with a prohibited person’s fraudulent use of an account and the confiscation of any winnings and things of value of a prohibited person.
11. Procedures for the logging in and authentication of an authorized participant in order to enable the authorized participant to commence sports betting and the logging off of the authorized participant when the authorized participant has completed play, including a procedure to automatically log an authorized participant out of the internet sports betting account after a specified period of inactivity.
12. Procedures for the crediting and debiting of an internet sports betting account.
13. Procedures for withdrawing funds from an internet sports betting account by the authorized participant.
14. Procedures for the protection of an authorized participant’s funds, including the segregation of an authorized participant’s funds from operating funds of the sports betting operator and/or internet sports betting platform provider.
15. Procedures and security measures to prevent ACH fraud regarding failed ACH deposits if an authorized participant’s internet sports betting account is funded through an ACH transfer.
16. Establishing policies and procedures with respect to credit.

**Section 5: Data Privacy and Security**

1. Procedures for the security and sharing of personal identifiable information of an authorized participant, funds or financial information in an internet sports betting account and other information as required by the board. The procedures must include the means by which a sports betting operator and/or internet sports betting platform provider will provide notice to an authorized participant related to the sharing of personal identifiable information.
2. Procedures and security standards to protect and respond to suspected or actual hacking or tampering by any person with the sports betting operator’s or internet sports betting platform provider’s internet sports betting website and sports betting devices and associated equipment.
3. Procedures to govern emergencies, including suspected or actual cyber-attacks, hacking, or tampering with the internet sports betting platform, internet sports betting website and sports betting devices and associated equipment. The procedures must include the process for the reconciliation or repayment of an authorized participant's internet sports betting account.

**Section 6: Responsible Gaming**

1. Detailed responsible gaming measures.
2. Method for securely implementing and using the information contained in the responsible gaming database.
3. Procedures for establishing and maintaining a self-exclusion list as prescribed in the act, rules, and direction of the executive director.
4. Procedures to prevent wagering by prohibited persons. Including processing winnings or things of value confiscated or withheld from a prohibited person.
5. Procedures for sports betting operator-imposed or internet sports betting platform provider-imposed exclusion of authorized participants, including the following:
	1. Providing a notification containing operator-imposed or internet sports betting platform provider-imposed exclusion status and general instructions for resolution.
	2. Ensuring that immediately upon executing the operator-imposed or internet sports betting platform provider-imposed exclusion order, no new wagers or deposits are accepted from the authorized participant, until such time as the operator-imposed or internet sports betting platform provider-imposed exclusion has been revoked.
	3. Ensuring that the authorized participant is not prevented from withdrawing any or all of his or her account balance, provided that the sports betting operator or internet sports betting platform provider acknowledges that the funds have cleared, and that the reason(s) for exclusion would not prohibit a withdrawal.

**Section 7: Test Accounts**

1. Procedures for test accounts must address the following:
	1. The procedures for the issuance of funds used for testing, including the identification of who is authorized to issue the funds and the maximum amount of funds that may be issued.
	2. The procedures for assigning each test account for use by only one individual. This does not preclude a sports betting operator from establishing a specific scenario or instance of test account that may be shared by multiple users provided that each user’s activities are separately logged.
	3. The maintenance of a record for all test accounts, to include when they are active, to whom they are issued, and the employer of the individual to whom they are issued.
	4. The procedures for the auditing of testing activity by the sports betting operator or internet sports betting platform provider to ensure the accountability of funds used for testing and proper adjustments to gross sports betting receipts.
	5. The procedures for authorizing and auditing out-of-state test activity.

**Section 8: Terms and Conditions**

1. All terms and conditions addressing all aspects of the internet sports betting operation including the following:
	1. Name of the party or parties with whom the individual is entering into a contractual relationship, including any licensee.
	2. Individual's consent to have the sports betting operator or internet sports betting platform provider confirm the individual’s age and identity.
	3. Rules and obligations applicable to the authorized participant including, but not limited to all of the following:
		1. Prohibition from allowing any other individual to access or use his or her internet sports betting account.
		2. Prohibition from engaging in internet sports betting activity unless physically present in Michigan or another jurisdiction authorized under a multijurisdictional sports betting agreement.
		3. Consent to the monitoring and recording by the sports betting operator or internet sports betting platform provider and/or the board of any internet sports betting communications and geographic location information.
		4. Consent to the jurisdiction of the State of Michigan to resolve any disputes arising out of internet sports betting.
		5. Prohibition against utilizing automated computerized software or other equivalent mechanism, such as a "bot," to engage in play.
	4. Full explanation of all fees and charges imposed upon an authorized participant related to internet sports betting transactions.
	5. Availability of internet sports betting account statements detailing the authorized participant’s internet sports betting account activity.
	6. Privacy policies, including information access.
	7. Legal age policy, including a statement that it is a criminal offense to allow an individual who is under the age of 21 to participate in internet sports betting.
	8. Full explanation of all rules applicable to dormant internet sports betting accounts.
	9. Authorized participant’s right to set responsible gaming limits and to self-exclude.
	10. Authorized participant’s right to suspend his or her internet sports betting account for a period of no less than 72 hours.
	11. Action that will be taken in the event an authorized participant becomes disconnected from the internet sports betting platform during game play.
	12. Notice that a malfunction voids all pays.
	13. Estimated time period for withdrawal of funds from internet sports betting account.
	14. Comprehensive house rules must address the following items regarding internet sport betting wagers, at a minimum:
		1. Types of internet sports betting wagers accepted.
		2. Minimum and maximum internet sports betting wagers.
		3. Description of the process for handling incorrectly posted events, odds, internet sports betting wagers, or results.
		4. Method for calculation and payment of winning internet sports betting wagers.
		5. Effect of schedule changes.
		6. Method of notifying authorized participants of odds or proposition changes.
		7. Acceptance of internet sports betting wagers at other than posted terms.
		8. Procedures related to pending winning internet sports betting wagers.
		9. Method of contacting the sports betting operator or internet sports betting platform provider for questions and complaints.
		10. Description of prohibited persons and events and wager types on which internet sports betting wagers may not be accepted under the act and these rules.
		11. Methods of funding a wager.
		12. Maximum payouts: however, such limits must only be established through limiting the amount of an internet sports betting wager and cannot be applied to reduce the amount paid to an authorized participant as a result of a winning internet sports betting wager.
		13. A policy by which the sports betting operator or internet sports betting platform provider can cancel internet sports betting wagers for obvious errors in accordance with the sports betting operator’s or internet sports betting platform provider’s internal controls, which must include a definition and procedures for obvious errors.
		14. Parlay wager related rules.
		15. Rules and procedures for wagering communications.
		16. Any other house rule related information the board determines necessary.