GOBIERNO DE PUERTO RICO

COMISIÓN DE JUEGOS DEL GOBIERNO DE PUERTO RICO

SPORTS BETTING MINIMUM INTERNAL CONTROL STANDARDS (MICS)

Section 1.0 Introduction: Minimum Internal Control Standards (MICS)

This document contains the Minimum Internal Controls Standards ("MICS") of the Puerto Rico Gaming Commission ("Commission") that apply to licensed Sports Betting Operators**.** However, the Commission, under its regulatory authority, requires the Operators to submit and ensure compliance with the MICS. The MICS are designed to provide a basic framework for Operators to establish and maintain a written system of internal control ("internal controls"). It is the Operator's responsibility to assure that their internal controls comply with the MICS. Operators must establish procedures that meet or exceed the requirements as set forth in the MICS.

The purpose of these MICS is to ensure all Operators apply the same minimal due diligence to their Sports Betting Operations in the Commonwealth, including procedures, administration, and accounting controls. Compliance with these MICS is to also ensure that Operators have appropriate security controls in place so that players are not exposed to unnecessary risks when choosing to participate in Sports Betting.

These MICS shall be included in and made a part of any Operator's sports betting operations. The Commission, from time to time, may amend these MICS and adopt new MICS. When this occurs, Operators shall be advised of these changes.

In the event of a conflict between the Law No. 81 of July 29, 2019, as amended, known as the Law of the Gaming Commission of the Government of Puerto Rico ("Law"), the Puerto Rico Sports Betting Regulations ("Regulations"), the MICS, and the adopted GLI-33 Standards for Event Wagering Systems ("GLI-33") as posted on the GLI website at www.gaminglabs.com, the Law will govern the Regulations, and the Regulations will govern the MICS and adoption of GLI-33.

Internal Auditors, External Auditors, Key Persons and employees of Operators are required to report violations of the internal controls to management and the Commission. Violations of the internal controls or the MICS may result in disciplinary action.

The Executive Director, by administrative approval, may exempt an Operator from compliance with any of these MICS. All requests for exemption must be in writing and state the justification for the exemption and proposed alternative methods, if any, the Operator will undertake to accomplish the stated purpose of these MICS.

Section 2.0 Internal Control Procedures

2.1. Internal Control Submissions

2.1.1. The Operator shall develop and submit to the Commission a comprehensive written system of internal control ("Internal Controls") that complies with the "Standards for Internal Controls" defined by the Regulations, as well as these MICS.

2.1.2. The internal control submission shall contain narrative (and diagrammatic where appropriate) representations of the internal controls to be utilized by the Operator as required by these MICS.

2.1.3. The internal control submission shall be accompanied by a written statement signed by the Operator's chief financial officer and either the Operator's chief executive officer or a licensed owner attesting that the system satisfies the "Standards for Internal Controls" as provided in the Regulations, as well as these MICS.

2.1.4. The Operator must designate to the Commission the individual responsible for internal control submissions, including the coordination of communications between the Commission and the Operator.

2.2. Changes to Internal Controls

2.2.1. The Operator shall submit to the Commission any proposed changes to its previously approved internal controls at least thirty (30) days before the change takes effect, unless the Commission instructs it in writing to do otherwise.

2.2.2. Each proposed change to the internal controls will be classified per category and each category must be submitted under separate cover with tracked changes. The categories are defined as follows:

a. Substantive: A change to the internal controls which affects the method of complying with the MICS.

b. Administrative: A change to the internal controls which is editorial, clarifies procedures or changes position descriptions or titles.

c. Deviation: A change to the internal controls that constitutes an exception to or variance from the MICS. A detailed explanation of the necessity to deviate from the MICS and the compensating controls must be included with the submission.
d. Emergency: A change to the internal controls that if not approved and implemented by a given date would negatively impact the internal controls or cause serious interruption to gaming activities. Emergency changes to the internal controls should be rare.
e. Audit Finding/Recommendation: A change to the internal controls based on an internal/external audit finding or recommendation. A copy of the page(s) relating to the audit finding or recommendation from the applicable final audit report issued by the internal/external auditors must be included with the internal control submission.

2.2.3. All added text must be underlined. All deleted text must be lined out.
2.2.4. Changes made to any form included in the internal controls must be redlined and explained. It is not necessary to redline the form if it is completely revised, however, a clean copy of the form with an explanation of why the form was revised must be provided.
2.2.5. Whenever changes to job titles are requested, a summary of the old position, new position and reason for the change must be provided under separate cover with the submission.
2.2.6. If the addition of information on a page causes text to be moved to the next page, that page must also be submitted. The clean pages submitted must be ready for insertion into the Operator's internal controls.
2.2.7. Operators must maintain a log of all internal control changes. At a minimum, the log must include the page number(s), revision date, effective date and internal controls Revision Number.
2.2.8. A MICS cross-reference to any change made to the internal controls must be included with each submission. The internal controls page number and paragraph number must be referenced next to each MICS standard.
2.2.9. When moving text, the location of the old text must be lined out and its new location must be noted. Any revision to the moved text must be redlined in the new location.
2.2.10. No Operator may change their internal controls until approved.
2.2.11. Emergency changes may be submitted at any time. Emergency submissions will be reviewed upon receipt and returned to the Operator if they do not constitute an emergency.
2.2.12. Any changes which are submitted as a result of an audit finding or recommendation must be submitted during the Operator's next scheduled submission period following the issuance of the auditor's final report, with a notation of the audit report date on the internal controls Revision Form.

2.3. Copies of Internal Controls

2.3.1. The Operator shall make available a current version of its Commission-approved internal controls, in hard copy or through secure computer access, to:
a. All key employees and/or mandatory functions; and
b. The Commission

2.3.2. The Operator shall maintain, in hardcopy or electronic form, all superseded internal controls together with the written representations required under the record retention policy, for at least five (5) years subsequent to the date the internal controls were superseded. Any subsequent modifications to the internal controls require a version with tracked changes and a final clean version.

Section 3.0 Organization Structure

3.1. Segregation of Duties

There shall be a policy to implement segregation of duties detailing the respective roles and responsibilities of the people in charge of critical processes that could impact the integrity of sports betting to ensure that no group has overall control in a way that could impact sports betting integrity without management oversight. The Operator shall set very clear work responsibilities in order to minimize mistakes, limit liabilities, and increase the amount of separation between related duties. Internal controls must ensure that all functions, duties, and responsibilities are adequately segregated, performed in accordance with sound practices by qualified personnel, and monitored to detect procedural errors and to prevent the concealment of fraud.

3.2. Organizational Structure

The Operator shall maintain an organizational structure that meets, at a minimum, the following criteria, aimed at preserving the integrity of the sports betting operation. Provided that it meets the minimum criteria required in these MICS, the Operator will be allowed to adapt its organizational structure to the needs of its own management style. The Operator shall submit its organizational structure to the Commission for approval within thirty (30) days after the Commission has made a request to that effect. The organizational structure proposed by the Operator must be approved by the Commission and will be governed by the following criteria:

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 areas of responsibility.
b. The segregation of incompatible functions so that no employee is in a position both to commit an error or to perpetrate a fraud and to conceal the 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.
d. Areas of responsibility which are not so extensive as to be impractical for one person to monitor.
e. Any other criteria that the Commission deems necessary to achieve compliance with the purposes of the Law, the Regulations and these MICS.

3.3. Mandatory Functions

3.3.1. **Functions and Supervisory Positions**

The Operator's internal controls shall describe, at a minimum, the following functions and supervisory positions, except that the Commission will retain the discretion to waive any of these requirements based on the channels in which the Operator accepts wagers.

a. The Operator shall be required to employ the personnel herein described in the operation of sports betting, regardless of the position titles assigned to such personnel by the Operator in its approved organizational structure. These MICS include general names for positions and forms. Specific titles and form names must be included in the Operator's internal controls.
b. Functions described in these MICS shall be performed only by persons having the appropriate knowledge and skill, as well as, holding the appropriate license required by the Operator's approved organizational structure to perform such functions, or by persons holding the appropriate occupational license required by the Operator's approved organizational structure to supervise persons performing such functions.
c. Supervision must be provided as needed for each function by a supervisor with authority equal to or greater than those being supervised. Internal controls must identify the supervisor in the function responsible for ensuring that the function is operating in accordance with established policies and procedures.
d. Each of these functions and supervisors shall be required to cooperate with, yet perform independently of, all other functions and supervisors.

3.3.2. **Accounting Function**

The Operator shall maintain an Accounting Function which must be independent from the Sports Betting Function.

a. The personnel of the Accounting Function (Accounting Personnel) shall be supervised by an employee holding an occupational license reporting to the executive level management of the Operator.
b. The Accounting Function shall be responsible for, without limitation, the following:
    i. Accounting controls;
    ii. The preparation and control of records and data;
    iii. The control of stored data, the supply of unused forms, and the accounting for and comparing of forms used in operations.;
    iv. The preparation of daily financial reports; and
    v. The reconciliation of accounts with Payment Service Providers (PSPs).
c. The Accounting Function shall be 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. Among other things, this function shall include, but not be limited to, a daily audit of the sports betting documentation, a daily audit of the cage accountability, document control and signature verification.

3.3.3. **Internal Audit Function**

The Operator shall maintain an Internal Audit Function either through a separate on-site function, or through the use of corporate internal audit, or through the outsourcing of this function.

a. The Internal Audit Function shall maintain its independence through an organizational reporting line that is outside the sports betting operation.
b. The Internal Audit Function must consist of Internal Auditors independent of the areas subject to audit (auditors internal to the operation, officers of the Commission, or an outside accredited organization may perform this function).
c. The Internal Audit Function shall be supervised by an employee having an occupational license reporting to the audit committee or other independent function.

d. The Internal Audit Function shall be responsible for auditing the compliance with the Wagering Procedures and Practices of GLI-33, these MICS, as well as to the Law and Regulations provided by the Commission and the prevailing internal controls, including 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.
   iii. Reporting instances of non-compliance with the internal controls.
   iv. Reporting of any material weaknesses in the internal controls to the appropriate position in the organization;
   v. Recommending improvements in the internal controls to eliminate any material weakness in the internal controls;

e. The method by which the Operator fulfills its requirements with respect to the Internal Audit Function shall be described in the Operator's organizational structure.

f. The Internal Audit Function shall operate with audit programs, which, at a minimum, address the MICS. Additionally, the function shall properly document the work performed, the conclusions reached, and the resolution of all exceptions. All such working papers and documentation shall be retained for a minimum of five years.

3.3.4. **Customer Service Function**

The Operator shall maintain a Customer Service Function which shall be located at a physical operating space or office, if not local to the Authorized Location

a. The Customer Service Function shall be supervised by an employee holding an occupational license reporting to the senior management of the Operator.

b. The Customer Service Function shall be responsible for, without limitation, the following:
   i. Assisting players with account inquiries;
   ii. Assisting players with technical difficulties connecting to or wagering on the Sports Betting System; and
   iii. Registering and trying to resolve player complaints and disputes.

c. The Customer Service Function shall be knowledgeable about the availability of compulsive play treatment or counseling, procedures for self-limitation, self-exclusion, etc., and able to provide that information on request.

3.3.5. **Sports Betting Function**

The Operator shall maintain a Sports Betting Function responsible for the conduct of sports betting in accordance with the established wagering rules, as well as the MICS and approved internal controls of the Operator;

a. The Sports Betting Function shall be supervised by an employee holding an occupational license endorsed with the position of Sports Betting Manager that is employed by the Operator;

b. The Sports Betting Function must verify that all wagering rules and disclaimers are displayed at all times or made readily available to the player upon request;

c. The personnel of the Sports Betting Function (Sports Betting Personnel) shall hold an occupational license and not perform any functions that are not included in their job descriptions submitted to and approved by human resources or equivalent function;

d. Each Authorized Location shall have a Sports Betting Manager present at all times when sports betting is taking place;

e. The Sports Betting Manager ensures that there is sufficient supervision, knowledge and training within the function to provide for the proper and fair conduct of sports betting and is responsible for the operations of sports betting and final approval of all odds established on any wager made pursuant to these MICS; and

f. The Sports Betting Manager shall immediately notify the Commission upon the detection of any person participating in sports betting who is:
   i. Engaged in or attempting to engage in or reasonably suspected of cheating, theft, embezzlement, collusion, money laundering, or any other illegal activity;
   ii. Involuntarily excluded; or
   iii. Voluntarily excluded.

g. Affected Sports Betting Managers shall be notified of any issues impacting the integrity of sports betting operations.

3.3.6. **Compliance Function**

The Operator shall maintain a Compliance Function who will be responsible for ensuring the Operator's ongoing compliance with the Regulations, and the Operator's approved internal controls, for managing change to the control environment and interacting with the Commission regarding any regulatory matters;

a. The Compliance Function shall be supervised by an employee holding an occupational license endorsed with the position of Compliance Officer or equivalent reporting to the General Manager or equivalent;
b. The Compliance Function shall be responsible for, at a minimum, the following:
    i. To monitor, audit and report on compliance with the Law, Regulations, MICS and the Operator's internal controls;
    ii. To co-ordinate operations with the Commission in respect of projects where Commission approvals and certifications are required;
    iii. To act as custodian over unit internal control manuals and operating methods;
    iv. Coordinating all amendments of approvals processed by the Commission;
    v. Oversee both internal and external audit disciplines; and
    vi. Perform such other functions as prescribed by these rules and the Operator's internal controls.
c. The Compliance Function may be responsible for maintaining the current status of all lists and disclosures addressed in these MICS, including:
    i. Key Employee certifications by reporting material changes;
    ii. Notifying the Commission of any material changes to the ownership or structure of the Operator as the change is contracted, and even if it remains conditional;
    iii. Notifying the Commission of compliance failures; and
d. The Compliance Function shall be responsible for responding to the Commission on progress with respect to any instructions issued by the Commission to the Operator.

3.3.7. **Information Technology (IT) Function**

The Operator shall maintain an Information Technology (IT) Function either through a separate internal function, or through the outsourcing of this function to a third-party IT Service Provider.

a. The IT Function shall be supervised by an employee holding an occupational license endorsed with the position of IT Director that is independent of the operation of the sports betting activity.
b. The IT Function shall be responsible for, without limitation, the following activities:
    i. The quality, reliability and accuracy of all computer systems used by the Operator in conducting sports betting operations, including the specifications of appropriate computer software and hardware.
    ii. Procedures for security, physical integrity, contingency, and maintenance of:
        1) Access codes and other data-related security controls used to ensure appropriately limited access to computers and the system-wide reliability of data;
        2) Computer tapes, disks, or other electronic storage media containing data relevant to sports betting operations;
        3) Computer hardware, communications equipment and software used in the conduct of sports betting operations; and
        4) Adequate backup and recovery procedures.
    iii. The acquisition, installation and maintenance of all hardware, software and data communications resources required to support sports betting operations;
    iv. The provision of physical and environment security designed to ensure that access to computer hardware and data communication equipment is limited to authorized personnel and to provide standard environmental components, including reliable electric service and appropriate temperature control;
    v. The timely back-up of information resources and the development of a contingency plan with all of the operator's functions, continually review the plan to ensure it remains current and compliant, and review the results of any test of the plan to ensure it is properly executed;;
    vi. The development and maintenance of access controls that limit the use of all information resources to authorized users and permit access only to the types of transactions and functions that authorized users are permitted to exercise;
    vii. The development of IT audit procedures and the preservation of audit data that enable the monitoring and investigation of unlawful, unauthorized, or inappropriate information system activity and ensure that these actions can be traced to the user(s) responsible; and
    viii. Maintaining current documentation with respect to the network topology (e.g., flowchart/diagram), deployment of server(s) housing application and database, and inventory of software and hardware deployed (available upon request by authorized internal and external auditors and by Commission

personnel). The employee responsible for maintaining the current documentation on the network topology is to be delineated in the internal controls.

c. The personnel of the IT Function (IT Personnel) having access to Sports Betting Systems may not have signatory authority over financial instruments (currency, winning wager tickets, vouchers, checks, etc.) and payout forms and must be independent of and restricted from access to:
   i. Financial instruments;
   ii. Accounting, audit, and ledger entries; and
   iii. Payout forms.

3.3.8. **Security Function**

The Operator shall maintain a Security Function that will be responsible for developing a security strategy in accordance with the overall operation. The Security Function at the Authorized Location shall employ licensed security officers. Nothing in these MICS shall prohibit the Operator from utilizing outside vendors for unrelated security functions.

a. The personnel of the Security Function (Security Personnel) who participate in any aspect of the sports betting operation shall at all times be employees of the Operator or be hired through an existing third-party agreement.
b. The Security Function shall be independent of the IT Function with regard to the management of security risk and all aspects of the operation of Sports Betting.
c. The Security Function shall have the competences and be sufficiently empowered and shall have access to all necessary resources to enable the adequate assessment, management, and reduction of risk.
d. The Security Function shall also be responsible for the security of the Authorized Location in all its aspects, including, but not limited to, the following:
   i. Collaboration with law enforcement;
   ii. The physical safety of players and employees in the Authorized Location, including during critical situations (e.g., active shooter, armed robbery), terror attacks or other threats or in the event of a fire or other emergency;
   iii. The physical safeguarding of assets transported to from, or through the Authorized Location and immediate notification to the Commission of any incident that has compromised the safeguarding of such assets;
   iv. The protection of the players, employees and Authorized Location property from illegal activity;
   v. The investigation of any person engaging in, or suspected of having engaged in, any potential illegal activities and the notification of the Puerto Rico Police Department and the Commission of such investigation, if deemed appropriate;
   vi. If required by the Commission, the control and maintenance of a system for the issuance of temporary credentials and authentication of such credentials;
   vii. The review of all processes regarding security aspects of the Operator, including, but not be limited to, the protection of information, communications, physical infrastructure, and wagering processes;
   viii. Ensuring the Authorized Location is constantly secure during normal operations and any emergencies due to malfunctioning equipment, loss of power, any natural disaster or any other cause;
   ix. The identification, monitoring and removal of any person who is one or more of the following:
      1) An individual under the age of 18 years;
      2) An intoxicated or impaired individual;
      3) An individual who is involuntarily excluded;
      4) An individual who is voluntarily excluded;
   x. The recordation in a security incident log of any and all unusual occurrences including the date, time, nature of the incident, resolution of the incident, persons involved in the incident, and the assigned Security Personnel.
   xi. The review and analysis of reports of unusual activity for evidence of fraud, collusion and cheating;
   xii. The immediate notification of appropriate supervisors and the Commission upon the detection of cheating, theft, embezzlement, or other illegal activities; and
   xiii. Acting as a “verifier” when required.
e. The Security Function will subsequently work with the other functions to implement the associated action plans. It shall be involved in reviewing all tasks and processes that are necessary from the security perspective for the Operator, including, but not limited to, the protection of information and data, communications, physical, virtual, personnel, and overall operational security.

f. The Security Function shall be supervised by an employee holding an occupational license endorsed with the position of Head of Security reporting to no lower than executive level management of the Operator. The Head of Security shall be responsible for recommending security policies and changes.

3.3.9. **Surveillance Function**

The Operator shall maintain a Surveillance Function for each Authorized Location which must be independent of all aspects of the operation of Sports Betting.

a. The personnel of the Surveillance Function (Surveillance Personnel) shall at all times be employees of the Operator. Operators shall not outsource the Surveillance Function to any third-party service provider, unless approved by the Commission;
b. The Surveillance Personnel shall be reasonably segregated and independent of all other personnel for the sports betting operation;
c. The Surveillance Personnel shall have prior approval of the Commission before transferring into a position that is not in the Surveillance Function the reverse applies as well;
d. The Surveillance Personnel shall be trained in the use of the CCTV System
e. The Surveillance Function shall be supervised by an employee holding an occupational license reporting to the property general manager, or to the license holder, or to a corporate executive outside the immediate property management team, or to another independent reporting line as approved by the Commission;
f. The Surveillance Function shall be responsible for the overall surveillance of the Authorized Location including, without limitation, the following:
    i. The sole control of all surveillance cameras;
    ii. The surveillance of the conduct and operation of the Kiosks, Ticket Writer Stations, and main cage;
    iii. The movement of cash or equivalent, player checks, winning wager tickets and vouchers, and any other Authorized Location assets;
    iv. The audio-video recording of activities in the count room;
    v. Detection of the presence in the Authorized Location of any person who is one or more of the following:
        1) An individual under the age of 18 years;
        2) An intoxicated or impaired individual;
        3) An individual who is involuntarily excluded;
        4) An individual who is voluntarily excluded;
    vi. Detection of cheating, theft, embezzlement, and other illegal activities in the Authorized Location;
    vii. The video recording of illegal, suspicious and unusual activities monitored; and
    viii. The immediate notification of appropriate supervisors and the Commission upon the detection and taping of cheating, theft, embezzlement, or other illegal activities.

3.3.10. **Main Cage Function**

The Operator shall maintain a Main Cage Function for each Authorized Location which may be separated into independent operations for Sports Betting and other activities.

a. The Main Cage Function shall be supervised by an employee holding an occupational license endorsed with the position of Cage Supervisor reporting to the supervisor of the Accounting Function or equivalent function;
b. The Main Cage Function shall be responsible for, without limitation, the following:
    i. The custody of cash or its equivalent, player checks, winning wager tickets and vouchers, and documents and records normally associated with the operation of a main cage;
    ii. The approval, exchange, and redemption of player checks received for the purposes of sports betting;
    iii. The control and supervision of all cages, ticket writers, cashiers, and the count room;
    iv. Such other functions normally associated with the operation of a main cage; and
c. The Main Cage Function must be independent of the count in respect of revenues from the Wagering Equipment.

3.4. Job Descriptions – Roles and Responsibilities

3.4.1. The Operator shall document their organizational structure, including job responsibilities by providing job descriptions for each supervisory and Key Employee position, containing the following information:

a. The role/objectives of the position;
b. Reporting relationships both internally and externally, including immediate supervisor;
c. Major duties, controls and responsibilities;
d. The titles/functions of the position(s), if any, which report to the post-holder;

e. Access to sensitive assets and areas;
f. Signatory ability, including alternate procedures in cases in which the required signatory is unable to perform their duty; and
g. The knowledge, skills, qualifications and experience required for the position.

3.4.2. As these roles form a critical part of the control environment, each Operator has a continuing obligation to notify the Commission of any changes to incumbents, job descriptions, and/or the responsibilities attached to a position prior to implementing any change in management or key personnel roles in writing within 24 hours

3.4.3. The Operator shall ensure that its employees conduct sports betting operations in a manner that does not pose a threat to the public health, safety, and welfare of Commonwealth residents.

3.4.4. The lowest job title of that function with the authority for that duty must be listed in the internal controls. Employees with higher authority within the same function may perform these duties, except where specifically noted in the internal controls. When a higher job title of that function performs the duties of a lower job title of that function, he/she may not then perform verification of his/her own work. A lower job title may be assigned the job duties of a higher job title within the same function for the operational day, provided that the assigned job title is within the same Commission Occupational License Badge Level. An employee temporarily working in the higher job title may not perform verification of his/her own work. Once assigned to the higher job title, the employee cannot return to his/her lower job title for the rest of the operational day. If employees are promoted to a key position in the company, they are deemed as qualifier and must undergo a higher level of due diligence

3.5. Staff Training

3.5.1. To mitigate the risk that untrained staff may bring to regulated operations by knowing or unknowing acts in violation of regulatory requirements, the personnel of the Operator shall be trained in all internal controls relevant to each employee's individual function.

a. Special instructional programs may be developed by the Operator in addition to any on-the-job instruction sufficient to enable all employees to be thoroughly conversant and knowledgeable with the appropriate and required manner of performance of all activities relating to their functions. The following subjects for training will contribute to an effective control environment:
   i. Anti-money laundering;
   ii. Responsible play and player protection, including but not limited to, definitions of key terms, myths and facts and where to get help, with content updated as necessary
   iii. Player verification and identification recognition;
   iv. Fraud and security awareness; and
   v. Regulatory controls to which the organization is subject.
b. A written description of all instructional and on-the-job training to be and being provided shall be made available to the Commission for review upon request. Training program information must include the following:
   i. The timeframe within which new employees are required to have completed the training;
   ii. Who is responsible for delivering the training;
   iii. How often the training is provided;
   iv. How the training varies depending on the nature of the employees' role; and
   v. How the effectiveness of the training is assessed.
c. Records shall be kept of all internal staff training and all employer-sponsored external training undertaken by employees to enable them to fulfill their roles, identifying who attended the training, what was covered, when the training took place and what the results were of that training. Training records shall be kept for a minimum of five years and shall be provided to the Commission upon request.

3.5.2. The training program must be undertaken by new personnel within one month of commencing work with the Operator but before interacting with a player about, or influencing, the provision of Sports Betting.

3.5.3. Employees interacting directly with players should be trained to ensure they understand compulsive play issues and know how to respond to them. These employees are taught skills and procedures specific to their position to respond to situations where a player is in distress. Employee knowledge of responsible play should be tested as part of the training.

3.5.4. Existing personnel who have undertaken the approved training program must undertake an annual refresher training course to refresh content knowledge and information on any recent changes in the above subjects, including player protection and/or responsible play.

3.6. Background Checks

3.6.1. The Operator shall conduct:

a. Background checks on newly hired employees engaged in activities related to the conduct of Sports Betting; and
b. Annual background checks on all existing employees engaged in activities related to the conduct of Sports Betting.

3.6.2. The background check must include a search for criminal history and any charges or convictions involving corruption or manipulation of Sports Events or Special Events and any association with organized crime.

3.7. Personnel Security

There shall be a policy and process for establishing trust in individuals that could impact the integrity of sports betting through security vetting. There shall be an associated policy and process for implementing monitoring of the system activity of personnel to detect and investigate activity that might impact sports betting integrity. These policies shall balance an individual's right to privacy with the obligation of the operator to protect the integrity of sports betting.

3.8. External Consultants

Details of any key external consultants must be included as part of the internal controls. This must identify their role within the business and the nature of their contractual relationship with the business where their ongoing involvement is critical to the business. The extent to which due diligence has been performed must also be recorded

3.9. Code of Conduct

3.9.1. The Operator shall have a suitable code of conduct documented in the internal controls and effectively implemented.

3.9.2. A code of conduct shall be issued to all employees when initially employed. All employees shall formally acknowledge acceptance of this code.

3.9.3. The code of conduct shall include statements that:
a. All policies and procedures are adhered to and that infringement or other breaches of the code could lead to disciplinary action.
b. Employees are required to declare conflicts of interest on employment as and when they occur. Specific examples of conflict of interest shall be cited within the code.

3.9.4. The code of conduct shall also address anti-graft provisions including hospitality and gifts provided by, or given to, persons or entities with which the Operator transacts business.

3.10. Signature Requirements

3.10.1. A "signature" on a document provides evidence of the person's involvement and/or authorization of the intentions reflected in these MICS. It is typically in the form of a stylized script associated with a person. The stylized script "signature" may include the first letter of the person's first name along with the person's full last name. The "initials" of the person would not meet the requirement of a "signature".

3.10.2. A system password is also acceptable as the "signature" of the employee authorizing a transaction through the Sports Betting System. An "electronic signature" is allowed only when being used as part of the Sports Betting System. The "electronic signature" is to be linked with an electronic document which identifies the individual entering the "signature". An "electronic signature" may also be attached to some biometric measurement. For instance, fingerprints or iris patterns are common biometric measurements.

Section 4.0 Systems and Components used for Sports Betting

4.1. Initial Certification

The Operator is responsible for ensuring all products deployed within the Commonwealth are certified by an independent testing laboratory in accordance to the standards set forth in GLI-33, these MICS, as well as to the Law and Regulations provided by the Commission and are accompanied by formal certification documentation noting as such.

4.2. Change Management Program (CMP)

4.2.1. The Change Management Program (CMP) shall be developed in accordance with the most current version of the GLI-CMP Change Management Program Guide as posted on the GLI website at www.gaminglabs.com

4.2.2. The Operator's CMP shall be approved by the Commission prior to its deployment and audited at an annual interval by the independent test laboratory.

4.2.3. The CMP's procedures and policies shall include policies for identifying criticality of updates and determining of submission of updates to an independent test laboratory for evaluation, which shall cover, at a minimum:
a. Maintenance of a source code repository of all system source code, containing snapshots of the complete system source code for each approved version of the Sports Betting System.

b. Documentation indicating the process in managing the development or modification of source code (available upon request by authorized internal and external auditors and by Commission personnel), including identification of the employee(s) responsible for said documentation
c. Documented method to ensure software is developed securely, following industry standards and/or best practices for coding and incorporating information security throughout the life cycle.
d. Processes for requests of new software or software changes. which must be reviewed by IT management. Approvals to begin work on the program are to be documented
e. Patching policies agreed upon with the Commission, whether developed and supported by the Operator or by the Technology Platform Provider.

4.2.4. Quarterly reports are issued to an independent test laboratory with knowledge of the product for review to ensure risk is being assessed according to the approved CMP and all documentation for all changes are complete.
a. The review consists of examining a sample of changes made during the prior period to determine whether:
i. The changes were properly approved at each of the development, testing and deployment stages;
ii. The changes were adequately documented and classified;
iii. The changes were properly tested, and any issues resolved; and
iv. Rollback procedures were applied as needed.
b. The evidence of the review is to be maintained and include at a minimum:
i. The date and time of the review,
ii. The name of the independent test laboratory who performing the review;
iii. The changes reviewed; and
iv. Any exceptions noted and any related follow-up on the noted exceptions.
c. A formal report shall be produced by the evaluating independent test laboratory noting the review as complete.

4.3. Annual Re-Certification

At least once annually, each product operating under a CMP must be fully certified to the standards set forth in GLI-33, these MICS, as well as to the Law and Regulations provided by the Commission and accompanied by formal certification documentation from an independent test laboratory with knowledge of the product. The Operator shall be allowed to seek approval for extension beyond the annual approval if hardship can be demonstrated. Granting of a hardship waiver is the sole discretion of the Commission.

Section 5.0 Security of Sports Betting Systems

5.1. Technical Security Controls

5.1.1. The Operator and/or Technology Platform Provider must adopt, implement, and maintain technical security controls that meet or exceed the Technical Security Controls of GLI-33, these MICS, as well as to the Law and Regulations provided by the Commission. These controls must be incorporated into the internal controls submitted to the Commission for approval.

5.2. System Integrity and Security Audit

5.2.1. An annual system integrity and security risk assessment shall be performed by an independent professional organization approved by the Commission to compliment the testing and annual certification designated for the Sports Betting System.

5.2.2. The system integrity and security risk assessment covers the applications transferring, storing or processing personally identifiable information (PII) or sensitive information, the underlying operating system, network components, and hardware changes not included in the evaluation of the Sports Betting System re-baselined. It is the responsibility of the Operator to coordinate with their Technology Platform Providers to ensure all critical components are audited.

5.2.3. The system integrity and security risk assessment on the production environment shall guarantee that no vulnerabilities putting at risk the security and operation of the Sports Betting System exist.

5.2.4. The Operator shall describe in the internal controls how the annual system integrity and security risk assessment will be conducted, including at minimum the following:
a. Review of the operational processes that are critical to compliance;
b. The processes for performing the vulnerability assessment and penetration testing
c. The processes for reviewing the firewall rules on all the perimeter firewalls and the internal firewalls to verify the operating condition of the firewall and the effectiveness of its security configuration and rule sets.
d. The process for communicating the results of system integrity and security risk assessment to the Commission no later than one month after the date of the scan or penetration test.

e. The process for addressing any recommendations contained in the system integrity and security risk assessment reports.

5.3. Sports Betting Asset Management

5.3.1. The internal controls shall include a Critical Asset Registry (CAR) describing all critical components of the Sports Betting System including hardware and software, that affect the functionality of the Sports Betting System or has an influence on how Personally Identifiable Information (PII) and other sensitive information is stored/handled by the system

5.3.2. Internal controls shall be in place to ensure that all assets housing, processing or communicating sensitive information, including those comprising the operating environment of the Sports Betting System and/or its components, are accounted for.

5.3.3. Assets shall be disposed of securely and safely using documented procedures

5.3.4. Prior to disposal or re-use, assets containing storage media shall be checked to ensure that any licensed software, as well as PII and other sensitive information has been removed or securely overwritten (i.e., not just deleted).

5.3.5. A record of the disposal of equipment or media shall be kept.

5.4. System Architecture

5.4.1. The Operator shall maintain a description of the overall Sports Betting System architecture, including security measures, to ensure the integrity of the secure storage and processing of data.

5.4.2. All security domains, points of access, and communication media for sports betting operations conducted are to be delineated in the internal controls.

5.4.3. Production networks serving the Sports Betting System and its critical components shall be segregated into security domains based on a risk assessment of the functions performed on each network. The risk assessment shall consider:

a. The devices and software deployed on each network, e.g. wireless devices, database servers, VOIP devices, remote desktop capability, etc.

b. The accessibility of the network from the public Internet;

c. The value and classification of the information stored or processed in the network.

d. The access control policy and access requirements for the applications on the network.

5.4.4. The boundaries between networks having different security domains shall be secured from outside traffic. Systems shall be configured to detect and report security-related events at security domain boundaries.

5.4.5. The Operator shall provide a layered approach to security within the production environment to ensure secure storage and processing of data. The architecture shall support the use of layered access controls to applications running on the network.

5.5. Physical and Environmental Security

5.5.1. The Operator must provide the Commission with information on the production datacenters, computer rooms, network operations centers, and other defined critical locations housing critical components of the Sports Betting System, including the location of staff (operator, service provider, datacenter operator if the datacenter is maintained by an independent third-party) for operation, service and maintenance of Sports Betting System and/or its components.

5.5.2. The locations housing critical components of the Sports Betting System must include internal controls which delineate the methods, processes and practices used in meeting the following at a minimum:

a. Redundant power sources to reduce the risk of data loss in case of interruption of power;

b. Adequate climate control and fire suppression equipment;

c. Adequate security mechanisms, such as traditional key locks, biometrics, combination door lock, or electronic key card system to prevent unauthorized physical access to areas housing critical components of the Sports Betting System.

5.5.3. Physical access to the locations housing critical components of the Sports Betting System, shall be restricted and adequately secured or monitored by personnel at all times. While this specification is risk based, in practice it shall require a minimum of an auditable multi-factor authentication process.

5.5.4. The administration of the electronic security systems, if used to secure locations housing critical components of the Sports Betting System, is performed by personnel independent of the Sports Betting Function.

5.5.5. The administration of the physical access security mechanism used to secure locations housing the sports betting critical components, such as keys, cards, or fobs, is performed by authorized IT Personnel.

5.5.6. Non-IT Personnel, including the Technology Platform Providers of the Sports Betting System's computer equipment, are allowed access to the locations housing critical components of the Sports Betting System only when authorized

and accompanied by IT Personnel and with continuous monitoring by IT Personnel during each access by IT Personnel or personnel independent of the function using such application.

5.5.7. A record of each access by non-IT Personnel is maintained and includes at a minimum:
- a. The name of the visitor(s);
- b. Time and date of arrival;
- c. Time and date of departure;
- d. Reason for visit; and
- e. The name of IT Personnel authorizing such access.

5.5.8. The locations housing critical components of the Sports Betting System may be located locally, within a single Authorized Location, or may be remotely located outside of the Authorized Location, at a hosting center with each location selected having adequate security, protections, and controls over the components.
- a. Each hosting center shall provide a description of the facility and services available, including the following:
  - i. Location description including:
    - 1) Floor plan;
    - 2) Reliability of power and telecommunications;
    - 3) Bandwidth availability;
    - 4) Compliance of server room to international standards;
    - 5) Redundancy of power and telecommunications feeds;
    - 6) Offline power capabilities (e.g. UPS and generator power);
    - 7) Refueling requirements of generators and fuel acquisition arrangements;
    - 8) Fire suppression system(s);
    - 9) Temperature and humidity control system(s);
    - 10) Procedures for switching to offline power; and
  - ii. Security description including:
    - 1) Perimeter boundary fences;
    - 2) Use of security guards (employees or contracted);
    - 3) Access controls;
    - 4) Alarm systems;
    - 5) Video surveillance coverage and storage;
    - 6) Monitoring of personnel access to sensitive areas;
    - 7) Anti-surveillance measures;
    - 8) Tenants; and
    - 9) Contractors in use for services such as cleaning and maintenance.
  - iii. Disaster recovery capabilities, testing, and auditing.
  - iv. Internal controls including:
    - 1) Visitor access procedures and controls;
    - 2) Maintenance and audit of access logs;
    - 3) Alarm procedures for technical and security response;
    - 4) Due diligence performed on contractors, tenants, and staff;
    - 5) Emergency access procedures; and
    - 6) Any other relevant procedures.
- b. The above requirement may be waived if the hosting center can demonstrate, to the satisfaction of the Commission, that the disclosure of certain information required above would hinder operations or pose a hardship due to contractual obligations.

5.6. Communications Security

5.6.1. The Sports Betting System 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 between any system components are performed across internet/public or third-party networks, the system shall either encrypt the data packets or utilize a secure communications protocol to ensure the integrity and confidentiality of the transmission.

5.6.2. All entry and exit points to the network shall be identified, managed, controlled, and monitored on a 24/7 basis. The Operator shall monitor all its Sports Betting Systems in order to prevent, detect, mitigate, and respond to cyberattacks.

5.6.3. Intrusion detection and reporting or an intrusion prevention system shall be in place on the networks and actively configured to notify system administrators.

5.6.4. In virtualized or cloud environments, each server instance may perform only one function. Alternative equivalently secure mechanisms will be considered as technology advances.

5.6.5. A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities. Telecommuting shall not be permitted except under circumstances where the security of the endpoint can be guaranteed.

5.6.6. If guest networks are offered (such as, networks that provide internet access for players, athletes or participants, or Suppliers), adequate logical segregation is provided of the guest network from the network used to serve access to sports betting related applications and devices. Traffic on guest networks is non-routable to the network serving sports betting related applications and devices.

5.7. Encryption and Cryptographic Controls

The internal controls shall describe how and where encryption or cryptography is used in the Sports Betting System to protect the confidentiality and integrity of PII and other sensitive information as appropriate. The following shall also be included in the internal controls:

a. The required level of protection of all PII and other sensitive information passed over networks based on a risk assessment and information classification.
b. The need for encryption of stored PII and other sensitive information on portable computer systems (end user devices e.g. laptops, removable media e.g. USB devices, and similar) and to protect the integrity of sensitive information held at rest on Wagering Equipment
c. Secure encryption keys in a way which limits access.
d. Integrity measures for the storage of winning wager ticket and voucher data and validation information.
e. The roles and responsibilities of IT Personnel for key management and the implementation of the cryptography policy.

5.8. Firewalls

The Sports Betting System must be equipped with a firewall which shall be able to record the audit information to preserve and secure the information from loss or alteration.

5.9. Third-Party Systems

The Operator is to document within their internal controls the policies and procedures for managing third parties who provide information security services, hardware, and/or software or interact with the system as well as the use of any additional third-party systems/processes that are not managed by the Operator, an example might be a third-party service provider who is contracted to perform patch management, system backups, or vulnerability testing. A third-party system is a hardware system or process performed by someone who is not part of the Operator or Technology Platform Provider, examples include a Commission managed to operate the physical computer system, perform backups, or provide security services. This would also include a technology firm who provides assurance services such as SOC audits. None of these need licenses but the Commission would like to understand the environment in which the Sports Betting operates.

5.10. Third-Party Data Processing

Unauthorized third-party service providers shall be prevented from viewing or altering PII and other sensitive information. Where PII and other sensitive information is shared with third-party service providers, formal data processing agreements shall be in place that states the rights and obligations of each party concerning the protection of the PII and other sensitive information. Each data processing agreement shall set out:

a. The subject matter and duration of the processing;
b. The nature and purpose of the processing;
c. The type of data to be processed;
d. How the data is stored;
e. The detail of the security surrounding the data;
f. The means used to transfer the data from one organization to another;
g. The means used to retrieve data about certain individuals;
h. The method for ensuring a retention schedule is adhered to;
i. The means used to delete or dispose of the data; and
j. The categories of data.

Section 6.0 Information Security Management System (ISMS)

6.1. ISMS Plan

6.1.1. The Operator or IT Service Provider shall implement, maintain, regularly review and revise, and comply with a comprehensive Information Security Management System (ISMS) plan, the purpose of which shall be to take reasonable steps to protect the confidentiality, integrity, and availability of personally identifiable information (PII) of

individuals who place a wager with the Operator, and shall contain administrative, technical, and physical safeguards appropriate to the size, complexity, nature, and scope of the operations and the sensitivity of the PII owned, licensed, maintained, handled, or otherwise in the possession of the Operator

6.1.2. The ISMS plan shall contain:

a. A commitment by management to actively support security and compliance within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of cybersecurity, information security and compliance responsibilities.

b. A description of how cybersecurity and information security roles and responsibilities of Operator personnel and relevant third-party service providers for the operation, service and maintenance of the Sports Betting System and/or its components.

c. A reference to the Technology Platform Provider's policies and procedures which support cybersecurity and information security activities within the organization.

d. A requirement for review at planned intervals and when changes occur to the Sports Betting System or the Operator's processes which alter the risk profile of the system

e. A requirement to communicate cybersecurity and information security policies to all employees and relevant third parties.

6.1.3. The ISMS plan shall also address:

a. The protection of PII and other sensitive information from unauthorized access;

b. The creation of required logs, with controls to prevent unauthorized modification; and

c. The existence of proper controls and documentation for changes and updates and patches to the Sports Betting System.

6.1.4. A security forum or other organizational structure comprised of senior managers, including the Head of Security or equivalent shall be formally established to monitor and review the ISMS to ensure its continuing suitability, adequacy and effectiveness, maintain formal minutes of meetings, and convene at least every six months.

6.2. ISMS Security Officer

The operator shall ensure that it has at all times an ISMS officer to assure day-to-day compliance and to be responsible for all areas of IT by the Operator. The ISMS officer shall:

a. Serve as the primary liaison to executive level management and the Commission for all matters regarding all aspects of cybersecurity and information security;

b. Have responsibility for the:

i. Evaluation of the operator's IT staffing levels and recommend any changes needed to ensure protection of the IT infrastructure;

ii. Creation of a standard for the proper segregation of IT job duties, including appropriate levels of account privileges;

iii. Evaluation of compliance with IT job segregation standards; and

iv. Development of IT security training for employees; and

v. Aspects of the operator's investigation and response to IT security related incidents.

c. Establish policies and procedures for monitoring employee access and ensuring deactivation of accounts assigned to terminated or suspended employees;

d. Approve the scope and review the results of any vulnerability scans and penetration tests. Review and approve resulting corrective action plans;

e. Be responsible for continual evaluation of all areas of the ISMS plan in order to ensure the plan is responsive to new security threats, laws, or regulations. Written procedures and internal controls shall be developed to address segregation of responsibilities, password administration, implementation of access controls and monitoring intrusions and security violations.

6.3. ISMS Audit

6.3.1. The ISMS shall undergo an annual audit against common cybersecurity and information security principles in relation to confidentiality, integrity and availability, as covered within these MICS. It is acceptable to leverage the results of prior audits conducted by appropriately accredited vendors and qualified individuals, within the current audit period (e.g., within the past year), against standards such as ISO/IEC 27001, the NIST Cybersecurity Framework, or equivalent. Such leveraging will be noted in the audit report.

6.3.2. An Operator making use of a virtualized or cloud environment, as allowed by the Commission, to store, transmit or process PII and other sensitive information shall undergo an annual audit against common cybersecurity and information security principles in relation to confidentiality, integrity and availability, as covered within these MICS. It is acceptable to leverage the results of prior audits conducted by appropriately accredited vendors and qualified

individuals, within the current audit period (e.g., within the past year), against standards such as ISO/IEC 27017 and ISO/IEC 27018 or equivalent. Such leveraging will be noted in the audit report.

6.4. ISMS Risk Management and Assessment

6.4.1. The ISMS officer shall create a risk management framework. In developing this framework, the ISMS officer shall:
- a. Utilize quantitative and qualitative based analysis to identify and rank all critical components of the Sports Betting System based upon risk;
- b. Document the criteria used to determine risk for each critical component of the Sports Betting System; and
- c. Establish minimum security standards for all critical components of the Sports Betting System based upon risk;

6.4.2. The internal controls shall describe how risk assessments are performed to identify, quantify, and prioritize risks against criteria for risk acceptance. The description of risk assessments shall include at a minimum:
- a. The methodology used for risk assessments, including:
  - i. A clearly defined scope for risk assessments; and
  - ii. A systematic approach for risk identification, and risk analysis.
- b. The manner in which risk assessments of Sports Betting components and operations are to be recorded and reported to management.
- c. The process for periodic reviews of the risk assessment.

6.5. ISMS Incident Management Procedures

6.5.1. Procedures must be implemented within the ISMS for responding to, monitoring, investigating, resolving, documenting, and reporting security incidents associated with the Sports Betting System.

6.5.2. The incident management process shall:
- a. Include a definition of what constitutes a security incident.
- b. Document how security incidents are reported through appropriate management channels.
- c. Address management responsibilities and procedures to ensure a rapid, effective and orderly response to security incidents, including:
  - i. Procedures to handle different types of security incident;
  - ii. Procedures for the analysis and identification of the cause of the incident;
  - iii. Communication with those affected by the incident;
  - iv. Reporting of the incident to the appropriate authority;
  - v. Forensic evidence collection; and
  - vi. Controlled recovery from security incidents.

6.5.3. The ISMS officer shall immediately inform the Commission and executive level management, including the IT Director, about all security incidents concerning:
- a. Unauthorized access to, or disclosure of, PII or other sensitive information;
- b. Unauthorized system modification by a third-party;
- c. Unauthorized destruction of regulated IT assets or data; and
- d. Any attack that compromises the availability or operation of any critical components of the Sports Betting System;

6.5.4. All security incidents must be responded to within an established time period approved by the Commission and formally documented.

Section 7.0 Maintenance of Sports Betting Systems

7.1. Monitoring of Critical Services and Critical Components

7.1.1. The Operator have documented within the internal controls a list of critical services to players that are required for the continued operation of sports betting, as well as the availability and resilience requirements of those services. The Sports Betting System shall be architected to meet those requirements.

7.1.2. All critical components of the Sports Betting System are to be operational in order for the Sports Betting System to operate and commence sports betting. The Sports Betting System shall detect and record information regarding the failure or non-operation of any component within the Sports Betting System. A log of this event shall be generated.

7.1.3. If an Operator becomes aware of a reproducible error in the Sports Betting System that relates to network security, data security, accurate placement, or recording or redemption of wagers, location detection, or otherwise calls into question the security and integrity of the Sports Betting System, the Operator shall notify the Commission immediately. Such notification shall include:
- a. A description of the error;
- b. Risks created or imposed by the error; and

c. Efforts being taken by the Operator to prevent any impact to the security and integrity of the Sports Betting System.

7.2. Logging

7.2.1. Logging facilities and log information shall be protected against tampering and unauthorized access.

7.2.2. Event logs recording user activities, exceptions, and cybersecurity and information security events shall be generated on each system component in order to monitor and rectify anomalies, flaws and alerts. All logs shall be stored and regularly reviewed in order to be presented as evidence.

7.2.3. Transaction logging shall be enabled on all databases.

7.3. Exception Reports

7.3.1. Exception reports shall be generated for significant events or alternations. The internal controls are to indicate the system's capability of producing an exception report (includes listing of specific report[s]) and to what extent this report provides specified information.

7.3.2. Significant events or alternations which shall be tracked include, but are not limited to:

a. Failed login attempts, including IP Address. If configurable by the system, parameters may be set so that only certain attempts are flagged for review (e.g., failed login attempts exceeding a certain number or failed login attempts to a specific address are flagged for review);

b. Program error or authentication mismatch;

c. Significant periods of unavailability of the Sports Betting System or any critical component of the Sports Betting System. A significant period may be any length of time when a transaction cannot be performed;

d. Large wins (single and aggregate over defined time period) in excess of a value specified by the Commission, including wager information;

e. Large wagers (single and aggregate over defined time period) in excess of a value specified by the Commission, including wager information;

f. Large financial transactions (single and aggregate over defined time period) in excess of a value specified by the Commission, including transaction information;

g. System voids, past-post voids, in-progress voids, past-post write, in-progress write, overrides, and corrections;

h. Changes to live data files occurring outside of normal program and operating system execution. Databases and operating systems are to be configured to monitor for and record manual edits and modifications made by users (not automatically by programs or operating systems) to data files and database tables belonging to the Sports Betting System;

i. Changes that are made to the download data library, including the addition, changing or deletion of software, where supported;

j. Changes to operating system, database, network, and application policies and parameters. Policies and parameters include, but are not limited to:

i. Audit settings (types of events that are monitored and logged);

ii. Password complexity settings (minimum length, maximum age, etc.);

iii. System security levels (AS/400, QSecurity);

iv. Point structure for player loyalty;

k. Changes to date/time on master time server;

l. Audit trail of information or initially recorded data changed by administrator accounts. Information logged, if configurable, is to include the events related to the functions described in the definitions of “system administrator” and “user access administrator”.

m. Changes to previously established criteria for an event (not including line changes for active events), such as odds, cut-off times, event data;

n. Changes to the results of a Sports Event or Special Event;

o. Changes to promotion and/or bonus parameters;

p. Adjustments to a Player Account balance;

q. Changes made to PII and sensitive information recorded in a Player Account;

r. Deactivation of a Player Account;

s. Negative Player Account balance (due to adjustments and/or chargebacks)

t. Irrecoverable loss of sensitive information;

u. Any other activity requiring user intervention or supervisory approval and occurring outside of the normal scope of system operation; and

v. Other significant or unusual events as deemed applicable by the Commission (the internal controls are to delineate what other events are to be logged).

7.3.3. Exception reports produced for the Sports Betting System for the significant events or alternations listed above shall include at a minimum:
   a. The date and time of the significant event or alteration;
   b. Unique transaction identifier;
   c. Identification of user(s) who performed and/or authorized the significant event or alteration;
   d. Reason/description of the significant event or alteration, including data or parameter altered;
   e. Data or parameter value prior to alteration; and
   f. Data or parameter value after alteration.

7.3.4. The internal controls are to delineate separately for each layer of the system (application, operating system, database and network, where applicable) whether the system is configurable, and to what extent the system is configurable, in tracking specified events.

7.3.5. Exception reports are reviewed on a daily basis for propriety of transactions and unusual occurrences. The review shall be aimed at providing reasonable assurance that:
   a. Users are only performing activities which have been explicitly authorized; and
   b. Possible threats facing the Sports Betting System are being assessed.

7.3.6. All noted improper transactions or unusual occurrences noted during the review of exception reports are investigated with the results documented.

7.3.7. The employee(s) responsible for reviewing the exception reports is (are) delineated in the internal controls.

7.3.8. Evidence of this review (e.g., log, checklist, notation on reports) must be maintained for 18 months following the completion of the review. The evidence is to include:
   a. The date and time of review;
   b. Name and title of person performing the review;
   c. The exception report reviewed;
   d. Any exceptions noted; and
   e. Follow-up and resolution of exceptions.

7.3.9. Compliance may involve the use of an automated tool that “flags” the events for the Sports Betting System and provides the person assigned to complete the review with notification.
   a. A record of the notification must include the date and time of the notification.
   b. Maintaining the notification for 90 days may serve as evidence of the review, provided that the date, time, name of individual performing the review of the exceptions noted, and any follow-up of the noted exception are documented in the notification or in a separate document maintained as required by this MICS.

7.3.10. IT Personnel who review the logs are independent of the system administration and user access administration functions and do not have system access to perform any administrative functions in the systems for which the logs are being reviewed. Alternatively, the Operator may designate an employee outside of the IT Function, provided that the employee is independent of the function using the system for which the logs are being reviewed.

7.3.11. If an IT Service Provider maintains and administers the Sports Betting System on behalf of the Operator:
   a. The review of the logs is to be performed by IT Personnel who are employees of the Operator; or
   b. If an automated tool is used, the notification is to be provided to IT Personnel employed by the Operator.

7.4. Requirements for System Verification

7.4.1. The internal controls shall include a mechanism for verifying that the components of the Sports Betting System in the production environment and the Mobile Apps or Sites made available for download by players from the live website are identical to those approved by the Commission. Provision shall be made for the verification mechanism to be run at the following times:
   a. On restart of the Sports Betting System;
   b. On the incorporation of changed components to the Sports Betting System following the CMP;
   c. On a scheduled period of not more than 24 hours as determined by the Executive Director; and
   d. At any time at the request of the Executive Director.

7.4.2. A failure of verification of any component of the Sports Betting System shall result in an alert being communicated to the Information Systems Officer and the Commission within twenty-four (24) hours.

7.5. Control Program Verification Listing

7.5.1. The Operator shall generate a Control Program Verification Listing of the critical control program components along with their corresponding digital signatures to ensure there have been no unauthorized modifications

7.5.2. Each item in the Control Program Verification Listing shall have a unique code, version number and identification characteristic sufficient to ensure that the Internal Audit Function will be able to inspect some or all components at any given time and determine whether they have deviated from the approved version.

7.5.3. A member of the IT Function will be assigned responsibility for changes to each item in the Control Program Verification Listing.

7.6. System Procedures

7.6.1. System documentation for all in-use components of the Sports Betting System (versions of application, database, network hardware, and operating system) shall be maintained, including descriptions of both hardware and software (including version numbers), operator manuals, etc.

7.6.2. The internal controls are to delineate appropriate measures to detect, prevent, mitigate and respond to common active and passive attacks. The Operator shall also have an established procedure documented in the internal controls to gather cyber threat intelligence and act on it appropriately.

7.7. Procedures for Maintenance

7.7.1. The Operator shall document the responsibilities of the IT Function for the maintenance of the components of the Sports Betting System. The documentation shall include:

a. The roles of IT Personnel in performing routine and non-routine maintenance on the components of the Sports Betting System.
b. The source of procedures for performing routine maintenance activities.
c. The records of the maintenance activities required to be kept.

7.7.2. Sports Betting System components shall be provided with adequate primary power

7.7.3. Sports Betting network equipment shall be correctly maintained to ensure its continued availability and integrity. The logs of all routers, switches, firewalls and other network appliances should be reviewed on a scheduled basis for any errors, or performance concerns.

7.7.4. Sports Betting communications records covering network lag, connection speeds, and communications outages should be reviewed on a regular basis and corrective action taken if any errors or performance concerns are detected.

7.8. User Access Controls

7.8.1. Access Control Policy

An access control policy shall be established and documented within the internal controls which shall be periodically reviewed based on business and security requirements for physical and logical access to the Sports Betting System and/or its components. The access control policy shall ensure that access to the following is restricted and secured:

a. System software and application programs;
b. Data associated with sports betting; and
c. Communications facilities, systems, and information transmissions associated with the Sports Betting System.

7.8.2. Provisioning of Access Privileges

A formal user registration and de-registration procedure shall be in place for granting and revoking access to the Sports Betting System and/or its components.

a. Procedures shall be in place to control the allocation of access rights to components of the Sports Betting System. The procedures should cover all stages in the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to the Sports Betting System.
b. The internal control shall describe the assignment of employee access and job responsibilities for various components of the Sports Betting System. Provisioning for user accounts consist of assigning application functions matching the employee's current job responsibilities, unless otherwise authorized by management personnel, to ensure adequate separation of duties
    i. The allocation of access privileges shall be restricted and controlled based on business requirements and the principle of least privilege.
    ii. Employees shall only be provided with access to the services or facilities that they have been specifically authorized to use.
    iii. Management shall review user access rights at regular intervals using a formal process.
c. A system administrator, management personnel, the IT Service Provider, or persons independent of the function being controlled, establish, or review and approve, user accounts for new employees and employees who transfer to a new function.
d. The transferred employees must have access appropriate for the new position only when the access for the previous position has been removed or disabled. Any previously assigned application function access for the employee's user account is changed to inactive (disabled) prior to the employee accessing their new user account for their role or position in a new function.

e. 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 resulting in noncompliance with one or more MICS. Additionally, the user account has a unique prefix/suffix to easily identify the users with multiple user accounts within one application.

f. The access provisioning process must be documented; documentation must evidence authorization by the appropriate management personnel, original user access and each subsequent change to user account; documentation must be maintained and made available upon request.

7.8.3. Logical Access Control

The Sports Betting System, including application software, shall be logically secured against unauthorized access by authentication credentials allowed by the Commission, such as passwords, multi-factor authentication, digital certificates, PINs, biometrics, and other access methods (e.g., magnetic swipe, proximity cards, embedded chip cards).

a. Any authentication credentials stored on the system shall be either encrypted or hashed to the cryptographic algorithms that meet current industry accepted standards, such as ISO/IEC 19790, FIPS 140-2, or equivalent.

b. A fallback method for resetting authentication credentials (e.g., forgotten passwords) shall be at least as strong as the primary method. A multi-factor authentication process shall be employed for these purposes

c. The system shall allow for system administrator notification and user lockout or audit trail entry, after 3 consecutive failed attempts at authentication. Multi-Factor Authentication shall be required to unlock the account.

d. Restrictions on connection times such as but not necessarily limited to session timeouts shall be used to provide additional security for high-risk applications, such as remote access.

7.8.4. User Access Functions

The range of functions available to each user shall be defined in conjunction with the process owner, the IT Function and the Security Function.

7.8.5. Password Requirements

Where passwords are used as an authentication credential, security parameters for passwords, if configurable, shall be at least 8 characters in length. The internal controls are to delineate whether the system is configurable for security parameters for passwords, and to what extent the system is configurable in meeting the above Password requirements.

7.8.6. User Authorization

Where user sessions are tracked for authorization, the user session authorization information shall always be created randomly, in memory, and shall be removed after the user's session has ended.

7.8.7. Administrative Access

The internal controls are to delineate the assignment of administrative access and function for various components of the Sports Betting System.

a. Access to administer the network, operating system, applications, and database security and system parameters is limited to:
   i. Supervisory and/or management employees of the IT Function; or
   ii. IT employees under the supervision of supervisory and/or management employees of the IT Function; or
   iii. Employees of Operators under the supervision of supervisory and/or management employees of the IT Function; or
   iv. Employees of IT Service Provider.

b. The Sports Betting System and its components being administered are enabled to log all administrative account's activity. Such logs are to be maintained and include time, date, login account name, a description of the event, the value before the change, and the value after the change.

c. Administrative access at the operating system level for all servers that support or are part of the Sports Betting System must be reviewed quarterly. Reviews are performed by personnel independent of the IT Function and include a complete review of all user accounts with administrative access. The reviewer performs the following:

i. Review all administrative groups and groups with elevated privileges to ensure membership is appropriate.
ii. Review the last login date and time for all administrative accounts to determine whether any "stale" accounts exist (e.g., users on extended leave or terminated IT employees remain active in the system).
iii. Review administrative accounts to ensure that passwords have been changed at least once every 90 days.
iv. Examine user list to determine whether IT Personnel utilize normal user accounts for regular use and administrator accounts for administrative functions.

d. Documentation of the results of the review is retained for a period of 18 months and includes the date, time, and name and title of the person performing the review.

e. At least annually, the Sports Betting System is reviewed by personnel independent of the individual who sets up or makes changes to the system parameters. The review is performed to determine that the configuration parameters are accurate and have not been altered without appropriate management authorization (e.g., verify the accuracy of the takeout % or flat fee to collect on sports betting activity and the awarding of points based on the dollar amount wagered). The system must also be tested, if possible, to further verify the accuracy of the configuration parameters (e.g., simulate activity to verify the accuracy of the takeout % or flat fee and to verify the accuracy of the amount of points awarded). The test results are documented and maintained.

7.8.8. Removal of Access Privileges

The access rights of employees to the Sports Betting System and/or its components shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

a. The user access administrator and/or system administrator, as applicable, must be notified immediately, but no less than within 24 hours, 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 administrator who must promptly disable/remove access rights to the system(s).

b. Upon notification, the administrator must change the status of the employee's user account from active to inactive (disabled) status within a reasonable period of time, established in the internal controls. The period of time for notification of the administrator is to be set such that it is unlikely that the terminated employee would gain access, remote or otherwise, within the notification period.

7.8.9. Generic Accounts

Generic accounts at the application level are prohibited unless user access is restricted to inquiry only functions.

a. The use of generic accounts shall be limited, and where used the reasons for their use shall be formally documented in the internal controls.

b. Generic accounts at the operating system level, if used, are configured such that:
i. The user is automatically brought to the application logon screen immediately upon logging into the operating system, and the user is logged out of the operating system automatically upon exiting the application; or
ii. The user is only granted access to the assigned application(s) for the user's current job responsibilities, and the user is precluded from executing unassigned applications or functions from the terminal desktop and is precluded from interactive access to the operating system through the proper security configurations.

c. The internal controls are to delineate the method used to secure generic accounts.

7.8.10. Service Accounts

Service accounts, if used, are utilized in a manner to prevent unauthorized and inappropriate usage to gain logical access to an application and the underlying databases and operating system.

a. Service account log-in and password information is restricted to a limited number of authorized employees. Suggested methods include:
i. Service accounts are configured such that the account cannot be used to directly log in to the console of a server or workstation;
ii. Service account passwords are to be changed at least once every 90 days, and immediately upon termination of system administrators.

b. The employee responsible for the documentation indicating the method used to prevent unauthorized and inappropriate usage of these service accounts (available upon request by authorized internal and external auditors and by Commission personnel) is to be delineated in the internal controls.

7.8.11. Default Accounts

User accounts created by default (default accounts) upon installation of any operating system, database or application are configured to minimize the possibility that these accounts may be utilized to gain unauthorized access to system resources and data.

a. The employee responsible for the documentation indicating the procedures implemented to restrict access through the use of default accounts (available upon request by authorized internal and external auditors and by Commission personnel) is to be delineated in the internal controls.

b. Any other default accounts that are not administrator, service, or guest accounts must be disabled unless they are necessary for proper operation of the system. If these accounts must remain enabled, the passwords are changed at least once every 90 days.

7.8.12. Test Accounts

The Operator shall set up test accounts to be used by commission or operator employees to test each of the various components and operations of the Sports Betting System in accordance with internal controls, which, at a minimum, shall address the following procedures:

a. The procedures for authorizing testing activity and assigning each test account for use;

b. 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;

c. The maintenance of a record for all test accounts, to include when they are active and to whom they are issued; and

d. The procedures for the auditing of testing activity to ensure the accountability of funds used for testing and proper adjustments to reports and records.

7.8.13. List of Accounts

System administrators maintain a current list of all enabled human or system accounts.

a. The employee(s) responsible for maintaining the list is to be delineated in the internal controls. The documentation includes, at a minimum, the following:
   i. Name of system (i.e., the application, operating system, or database).
   ii. The user account login name.
   iii. A description of the account's purpose.
   iv. A record (or reference to a record) of the authorization for the account to remain enabled.

b. The current list is reviewed by IT management in addition to the system administrator at least once every six months. The internal controls are to delineate the employee(s) responsible for the review. The list is reviewed to perform necessary procedures:
   i. To identify any unauthorized or outdated accounts;
   ii. To ensure that all service, generic, and default accounts are not enabled for remote access;
   iii. To determine that the method used is a properly designed control process and is effectively operating to secure the generic, service, and default accounts from unauthorized usage.

c. If an IT Service Provider is used, the system administrator (the employee[s] delineated in the internal controls) maintains an additional list of all user accounts with system administrative permission which includes at a minimum:
   i. Name of the system administered by an IT Service Provider, and
   ii. The user account(s) login name(s) used by an IT Service Provider.

d. The current list required by (c) is are reviewed by IT management, in addition to the system administrator, at least once every six months. The internal controls are to delineate the employee(s) responsible for the review. The list is reviewed to ensure that the permissions are appropriate for each user's position.

7.8.14. User Access Listing

A User Access Listing must be maintained either manually or by systems that automatically record access changes and force authentication credential changes.

a. The written internal controls are to indicate the system's capability of producing a user access listing and to what extent the system's listing provides specified information. The User Access Listing may be archived electronically if the listing is written to unalterable media (secured to preclude alteration). If available, the list

of users and user access for a Sports Betting 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 Commission.

b. The User Access Listing shall be reviewed quarterly by personnel independent of the authorization and user provisioning processes.

i. The review consists of examining a sample of at least 10% (with a maximum of 25) of the users included in the listing. For each of the randomly selected users, the reviewer shall determine whether:

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

2) The assigned functions provide an adequate segregation of duties;

3) Terminated employees' user accounts have been changed to inactive (disabled) status within the time period determined by management and delineated in the internal controls. Verification of the time period is not required if the system is not capable of providing a user access listing indicating the date and time of an account being disabled/deactivated. The written internal controls are to delineate this reason for not performing a verification of time period;

4) Passwords have been changed within the last 90 days. The review for password changes within 90 days applies regardless of whether the system parameter has been configured to have the password changed at least once every 90 days. However, the review does not apply when the system is not capable of providing a user access listing indicating the date of the last password change. The internal controls are to delineate this reason for not performing a review for password changes.

5) There are no inappropriate assigned functions for group membership, if applicable. This applies to a review of the assigned functions for the selected user account with group membership.

ii. The reviewer must maintain adequate evidence to support the review process for the last four quarterly periods. The evidence is to include at a minimum:

1) The date and time of review;

2) The individual(s) performing the review;

3) The selected user accounts reviewed;

4) Documentation of the results of the review, including any exceptions, follow-up and resolution of exceptions.

7.8.15. User Access Logging

All actions performed on the Sports Betting System by human or system accounts shall be logged, and these logs shall be monitored, regularly reviewed, and acted upon as appropriate.

7.9. Remote Access to the Sports Betting System

7.9.1. Remote access allows a user access to the Operator's network from outside of this network through some form of a data link. Remote access typically involves the use of the Internet, a dial-up modem, and/or Virtual Private Network (VPN) or similar technology. A procedure for strictly controlled remote access shall be established and documented in the internal controls.

7.9.2. Remote access to any component of the Sports Betting System shall be configured to prevent the transfer of PII outside of the United States, unless authorized by the Commission.

7.9.3. Remote access to the Sports Betting System components (production servers, operating system, network infrastructure, application, database and other components) shall be limited to authorized IT Personnel employed by the Operator, except in the following cases:

a. Remote access by Provider personnel to any component of the Sports Betting System is allowed for purposes of support or updates and is enabled only when approved by authorized IT Personnel employed by the Operator. If the remote access to a database is performed by unlicensed Provider personnel, the remote access must be continuously monitored by IT Personnel employed by the Operator.

b. The Operator shall provide the Commission remote access to wagering transaction and related data as deemed necessary by and in a manner approved by the Commission.

7.9.4. Remote access may be allowed for non-IT Personnel (management personnel or other authorized employees of the Operator), however:

a. Non-IT Personnel must be precluded from directly accessing any databases or operating systems of any of the Sports Betting System and other production environment servers.

b. Additional security methods must be employed beyond passwords for user accounts to ensure that the Sports Betting System application and data integrity are maintained and secure. These additional security methods are to be delineated in the internal controls

7.9.5. Remote access to Player Accounts by authorized employees of the Operator from outside of the United States is allowed for the purposes of providing customer service but must be conducted via a remote desktop application to prevent the transfer of data from the application environment to the remote site. Access must be limited to only the application functions necessary for personnel to perform their job duties.

7.9.6. Provider accounts must be restricted through logical security controls to have the ability to access only the application(s) and/or database(s) that are necessary for the purposes of support or providing updates/upgrades.

a. The Operator must employ security methods in addition to passwords to verify the identity of Provider personnel prior to authorizing any remote access for that Provider

b. User accounts used by Providers must remain disabled on all operating systems, databases, network devices, and applications until needed by such Provider.

c. Subsequent to an authorized use by a Provider, the account is returned to a disabled state.

7.9.7. Any instance of remote access to Sports Betting System components shall be automatically recorded by a device or software in a remote access activity log.

7.9.8. For at least one day each quarter, the remote access activity log shall be reviewed by the Internal Audit Function.

a. The internal controls are to delineate the procedures and documentation used to perform the review.

b. The review is to reasonably assure:

i. Each remote access session by a Provider has been appropriately documented;

ii. Each remote access by non-Provider personnel (IT employee, management personnel, or other authorized employee) is performed by an individual who has been authorized to have such access.

c. Evidence of the review of remote access activity logs is to be maintained for the last four quarterly periods. The evidence is to include at a minimum:

i. The date and time of review;

ii. Name and title of person performing the review;

iii. The remote access activity log reviewed; and

iv. Any exceptions, follow-up and resolution of exceptions.

7.10. Software Downloads

7.10.1. Downloads must use secure methodologies that will deliver the download data without alteration or modification.

7.10.2. Downloads conducted during operational periods must be performed in a manner that will not affect Sports Betting.

7.10.3. Downloads must not affect the integrity of locally stored data.

7.10.4. The Operator must be capable of recording for each download:

a. The time and date of the initiation of the download;

b. The time and date of the completion of the download;

c. The system components to which software was downloaded;

d. The version(s) of download package and any software downloaded. Logging of the unique software signature will satisfy this requirement;

e. The outcome of any software verification following the download (success or failure); and

f. The name and identification number, or other unique identifier, of any individual(s) conducting or scheduling a download.

7.11. Backup and Recovery Procedures

7.11.1. Daily backup and recovery procedures shall be in place and shall follow a process documented in the internal controls.

7.11.2. Backup system logs are reviewed daily by IT Personnel or individuals authorized by IT Personnel to ensure that backup jobs execute correctly and on schedule. The backup system logs are maintained for the most recent 30 days. The employee(s) responsible for reviewing the backup logs is to be delineated in the internal controls.

7.11.3. Backup data files and data recovery components must be managed with at least the same level of security and access controls as the Sports Betting System for which they are designed to support.

7.11.4. The employee responsible for the documentation indicating the procedures implemented for the backup processes and for restoring data and application files (available upon request by authorized internal and external auditors and by Commission personnel) is to be delineated in the internal controls.

7.11.5. Quarterly, IT Personnel test the recovery procedures. A record is to be maintained indicating the date a test of the recovery procedures was performed and the results of the recovery test. Recovery procedures must include, but are not limited to, the following:

a. Data backup restoration;

b. Program restoration; and
c. Redundant or backup hardware restoration.

7.12. Contingency Plan

7.12.1. The Operator shall provide and annually update and test a Contingency Plan to recover sports betting operations if the Sports Betting System's production environment is rendered inoperable or in the event of a system hardware or software failure or other event resulting in the loss of system data. Such plan shall consider disasters including, but not limited to, those caused by weather, water, flood, fire, environmental spills and accidents, malicious destruction, acts of terrorism or war, and contingencies such as strikes, epidemics, pandemics, etc.

7.12.2. Utilization of virtualized or cloud environments for this purpose will be evaluated on a case-by-case basis;

7.12.3. The Operator shall include a process for testing the Contingency Plan at least annually.

a. A report detailing the results of the annual test shall be forwarded to the Executive Director no later than one month after the completion of the test.
b. A process for implementing any recommendations for improvement resulting from the annual test shall be documented.

7.12.4. The roles and responsibilities of the IT Personnel responsible for maintaining the contingency plan shall be documented in the internal controls.

7.12.5. The Operator shall furthermore plan, perform, and evaluate contingency exercises in regular intervals to prepare the Operator for crisis situations, covering the elements included in the contingency plan

Section 8.0 General Operating Procedures

8.1. Protection of Unpaid Funds

To secure funds related to honoring unpaid winning tickets and vouchers before and after the end of the redemption period, the internal controls must be established, and procedures implemented:

a. To ensure the validity of winning tickets and or vouchers redeemed and to verify that the player is paid the appropriate amount;
b. To document the payment of a claim on a ticket/voucher that is not physically available or a ticket/voucher that cannot be validated such as a mutilated, expired, lost, or stolen ticket/voucher;
c. Ensuring that each redeemed ticket or voucher shall not have the ability to be redeemed again;
d. Specifically related to the protection of funds related to unpaid winning tickets and vouchers and data files containing information relating to the payout status of each winning ticket and voucher, the specific winning tickets and vouchers with amounts owed but unpaid and the validation files
e. To handle the redemption of a winning ticket or voucher should the Sports Wagering Facility be closed;
f. To cover the entire period for honoring winning wagers and cashing out vouchers as well as the auditing of the final transfers upon wager settlement and voucher redemption;
g. That ensure the security of redeemed tickets and vouchers and the integrity of records of outstanding tickets;
h. Confirming the rules covering winning ticket and voucher validity time, payout on lost and defaced winning tickets and vouchers, inquiries into the validity of claims and late or last-minute payouts;
i. Confirming that access control be strict and limited to that required in respect of records of unpaid winning tickets and vouchers;
j. Confirming a reporting process in case of unauthorized access attempts;
k. Confirming an escalation process for any incident or suspicious activity; and
l. Confirming audit trails are able to identify unusual patterns of late payouts.

8.2. Operator to Player Communications

The Operator shall have internal controls in place for handling communications between them and the player, including maintaining chat logs and email correspondence for a period of ninety days or as required by the Commission.

8.3. Advertising

The Operator shall maintain internal controls which meet the Regulations for "**Advertising**". It is also strongly encouraged that the internal controls for advertising cover the items listed within the "**Responsible Marketing Code for Sports Betting**" posted on the American Gaming Association (AGA) website at www.americangaming.org.

8.4. Responsible Play

8.4.1. The Operator shall submit a Responsible Play Plan submitted to the Commission at the time of first application. The plan must be approved by the Commission prior to the commencement of sports betting activity. The Operator shall

resubmit their Responsible Play Plan for approval within ten (10) business days of any changes to the plan and at license renewal. The Plan shall include, at a minimum

a. The goals of the plan, procedures and deadlines for implementation of the plan
b. The identification of the individual(s) who will be responsible for the implementation and maintenance of the plan
c. A plan for providing comprehensive responsible training to employees who may interact with players, including annual or periodic refresher training. Training should equip the trainee to respond to circumstances in which gambling activity may indicate signs that are consistent with gambling addiction
d. The duties and responsibilities of the key employees and sports betting employees designated to implement or participate in the plan
e. An estimation of the cost of development, implementation and administration of the Responsible Play Plan.

8.4.2. The Operator shall establish procedures within their internal controls to promote responsible play. It is strongly encouraged that the internal controls to promote responsible play cover the items listed within the "**Responsible Gaming Code of Conduct**" posted on the American Gaming Association (AGA) website at www.americangaming.org.

8.4.3. The Operator shall have clear policies in place:

a. To monitor player activity for signs or triggers of compulsive play; and
b. For assessing and handling situations where a player indicates they are in distress or experiencing problems.

8.5. Prevent Extension of Credit or Promotion Thereof

The Operator shall have procedures to prohibit an Operator, director, officer, owner, and employee of the Operator from extending credit to an individual, group of individuals, or entity that places wagers with the Operator or seeks to place wagers with the Operator.

a. Credit providers such as small amount credit contracts (payday lending) must not be advertised or marketed to players.
b. A player must not be referred to a credit provider to finance their sports betting activities.
c. PII related to a player must not be provided to any credit provider.
d. The Operator shall neither extend credit to a player nor allow the deposit of funds into a Player Account that are derived from known extensions of credit by credit providers, affiliates or agents of the Operator.

Section 9.0 Authorized Sports Betting

9.1. Wagers on Sports Events and Special Events

9.1.1. The framework in which the Operator offers sports betting and the wagering rules shall be defined, maintained, and published, including but not limited to, all authorized events and wager types for each Sports Event or Special Event.

9.1.2. Unless otherwise stated within the "Authorized Sports Betting" section of the Regulations, wagering is permitted on all Sports Events and Special Events organized or sanctioned by any Sports Governing Body or equivalent that appears on the Commission's Authorized Sports Events and Special Events, Leagues and Wagers list.

a. This also includes, but is not limited to wagers which are related to:
    i. Any occurrence related to the conduct of a Sports Event and Special Event (e.g., coin flip to start a competition, length of a half-time show, etc.);
    ii. Individual athlete or participant performances in ancillary events (e.g., individual performances at a league combine, individual performances at skills competitions, or other Special Events, etc.);
    iii. Conduct or outcome of professional league drafts (e.g., which team will receive the first overall pick in a draft, which athlete will a team draft, etc.). Wagers related to each round of the draft must cease upon the commencement of that round; and
    iv. Any award granted or recognized by the Sports Governing Body or equivalent (e.g., athlete of the year, coach of the year, most valuable athlete, etc.). Wagers related to each award must cease prior to the award's announcement. In addition, if voters consist of individuals outside the scope of the integrity policy of the Sports Governing Body or equivalent, then it must be demonstrated to the Commission that the voting for such awards is collected and tallied:
        1) By individuals covered under their integrity policy or an independent third-party required to maintain the confidentiality of the outcome of the award until it is announced; or
        2) In a manner that maintains the confidentiality of the outcome until the award is announced.
b. However, this excludes wagers which are related to:
    i. Injuries (e.g., will an athlete or participant suffer an injury, how any games will an injured athlete or participant miss, etc.);
    ii. Officiating calls (e.g., when will the first penalty flag be thrown, when will the first foul be called, what will be the game's first penalty, etc.); and

iii. Other unsportsmanlike conduct.

9.1.3. Any Operator may petition the Commission for approval of a new event upon which Wagers may be placed or accepted. If an Operator would like to offer a new category of event or wager type, they must submit a request to the Commission using the Category of Sports Betting Request Form at least fourteen (14) days in advance of the proposed date of accepting wagers on such category of event or wager type.

a. A proposed new event may be a variation of an authorized Sports Event or Special Event, a composite of authorized events, or any other event compatible with the public interest and suitable for Operator use.

b. A Category of Sports Betting Request Form shall include the following information:

i. The name of the petitioner;

ii. Whether the new event or wager type is a variation of an authorized Sports Event or Special Event, a composite of authorized event or wager type, or any other event or wager type compatible with the public interest and is suitable for Operators use;

iii. A complete and detailed description of the new event or wager type for which approval is sought, wagering rules, and the manner in which wagers would be placed, payout information, source of the information used to determine the outcome of the sports wager, and any restrictive features of the wager

iv. A full description of any technology which would be utilized to offer the new event or wager type;

v. Information or documentation which demonstrates that the granting of the request for approval would be consistent with the public policy of the Commonwealth;

vi. Request for a test of the new event or wager type;

vii. Evidence of the independent integrity monitoring of the new Sports Event or Special Event or the integrity policy of the Sports Governing Body or equivalent; and

viii. Any other pertinent information or material requested by the Commission

c. The decision whether to grant approval to accept wagers on a new event or wager type shall be based on all relevant information including, but not limited to, the factors above. The Commission may subject any technology that would be utilized to offer the event to such testing, investigation and approval process as he deems appropriate.

9.1.4. The Executive Director shall approve, deny, or request further information within fourteen days of submission. If the Executive Director takes no action within that period, the operator may offer the requested Sports Betting unless the Executive Director issues a subsequent disapproval.

a. Upon approval of the new event or wager type, the Commission shall provide public notice of such approval including any conditions and limitations placed on such approval. Thereafter, any operator may accept wagers pursuant to the approval and any conditions and limitations placed thereon unless the wager type is subsequently disapproved by the Executive Director for any reason the Commission deems appropriate.

b. Except as otherwise provided in this subsection, any new event or wager type shall not be approved unless the Commission has acknowledged evidence of appropriate policies and procedures of the Sports Governing Body or equivalent to monitor the integrity of the athletes or participants, or independent integrity monitoring of the underlying Sports Event or Special Event upon which the new type of Sports Betting is based. In the absence of such acknowledgement, the Commission may allow for Sports Betting to occur, however will require the operator to impose a wager limit of not more than $100 and a win limit of $500 on such events.

9.2 Wagering Periods

A Wager can only be placed on a given Sports Event or Special Event if the wagering period is open. Employees authorized to manually open or close a wagering period shall be formally defined in the internal controls. Internal Controls shall ensure wagers are only accepted from players during the wagering period.

9.3 Placement of wagers

All wagers must be transacted through the Sports Betting System and processed in the order they are received. In case of system failure, no wagers may be manually placed.

9.4 Pre-Play Wagering

Pre-play wagers must be placed prior to the start time of the Sports Event or Special Event. At the discretion of the Operator as indicated in their internal controls, pre-play wagers may be accepted after the start time of the event if the final result is not known and no athlete or participant has achieved a material advantage (such as, but not limited to, scoring a goal or touchdown or expulsion of an athlete) at the time the pre-play wager is placed.

9.5 In-Play Wagering

There shall be documented procedures to assure and monitor the integrity of in-play wagering, the results handling and player protection. Indicative areas for consideration in the procedure for results handling shall include, but not be limited to, time delays, sources of results, and reversal of results. The procedures shall also account for courtsiding prevention mechanisms including but not limited to a delay in live pictures.

9.6 Wager Cancellations and Voids

9.6.1 Wagers cannot be modified except to be voided or cancelled as provided for in the Operator's published cancellation policy and in their internal controls.

9.6.2 A cancellation grace period may be offered to allow players to request a cancellation of wagers placed.

a. Player initiated cancellations may be authorized in accordance with the cancellation policy.
b. Any cancelled wager shall be refunded upon request by a player.

9.6.3 A Sports Betting System shall be configured to void and cancel wagers. A wager shall not be declared void or cancelled in the system without the approval of a supervisory employee of the Operator.

9.6.4 The internal controls shall delineate how the Operator reserves the right to void or cancel any wager and refuse to pay any prizes or recover any prizes already paid at any time for any reason, including if

a. A player used funds that were incorrectly credited to their Player Account to purchase the wager.
b. The outcome of the event is known or a material advantage has occurred, regardless of its outcome.
c. An in-play wager has been placed after the outcome of the event wagered on is known or an athlete or participant has achieved a material advantage (e.g., scoring a goal or touchdown or expulsion of an athlete).
d. The Operator cannot satisfactorily determine the Event Results only as provided in the Wagering Rules.
e. The Operator determines a player placed the wager illegally or otherwise violated the Wagering Rules.
f. The Operator has reasonable basis to believe there was obvious error in the placement or acceptance of the wager. Those errors include, but are not limited to:
    i. The wager was placed with incorrect statistical data;
    ii. Human error in the placement of the wager;
    iii. The wager ticket does not correctly reflect the wager; or
    iv. Equipment failure rendering a wager ticket unreadable.

9.6.5 The Operator shall also cancel a wager under the following circumstances:

a. Any wager where a Sports Event or Special Event which the subject of the wager is cancelled, or postponed or rescheduled to a different date prior to completion of the event;
    i. In the case of a wager on a portion of an event, that wager shall be valid when the event is canceled, postponed, or rescheduled if the outcome of the affected portion was determined prior to the cancelation, postponement or rescheduling.
    ii. The Operator may establish a timeframe in which an event may be rescheduled or postponed without canceling the wager. This timeframe shall be tied to specific events, subject to the approval of the Commission, and documented in the internal controls.
b. Any wager when an individual athlete or participant fails to participate in an event and the outcome of the wager is solely based upon that one individual's performance;
c. When ordered by the Commission pursuant to these MICS.

9.6.6 The Operator shall prevent the voiding or cancellation of wagers after the outcome of an event is known without the prior approval of the Commission.

a. The Operator may request the Commission to order the cancellation of all wagers of a specific type, kind, or subject. A request to cancel shall be in writing, and contain the following:
    i. A description of the type, kind, or subject of wager the Operator is requesting to cancel;
    ii. A description of any facts relevant to the request; and
    iii. An explanation why cancelling the wagers is in the best interests of the Commonwealth or ensures the integrity of the sports betting industry.
b. No wager subject to the request to cancel shall be redeemed until the Commission issues an order granting or denying the request to cancel.
c. If the Commission grants the request to cancel, the Operator shall make commercially reasonable efforts to notify players of the cancellation along with a reason for cancellation

9.6.7 The Operator shall cancel a wager made by a Prohibited Player and refund the amount wagered. The Operator must cancel a wager at the time the Operator becomes aware or should have been aware that the player is a Prohibited Player.

9.7 Winning Wager Ticket and Voucher Payment

9.7.1 Payment of Winnings

A Sports Betting System shall be configured to pay winning wagers and must be restricted to prevent unauthorized access and fraudulent payouts by one person.

a. Internal controls must be established, and procedures implemented that address the following:
   i. Identification of the employee authorized (by position) to make a payout;
   ii. Predetermined payout authorization levels (by position); and
   iii. Documentation procedures ensuring separate control of the cage accountability functions.

b. Upon scanning the wager ticket/voucher, the Sports Betting System brands the wager ticket/voucher with a paid designation, the amount of payment and date. Alternatively, if an employee manually enters or scans the wager ticket/voucher number into the Sports Betting System, the employee either immediately writes/stamps the date, amount of payment and a paid designation on the player's wager ticket/voucher or attaches to the player's copy a "paid" wager ticket/voucher which indicates a paid designation, the wager ticket/voucher number, the amount of payment and date.

9.7.2 Withholding Delinquent Child Support from Winnings

The Operator shall prepare and submit quarterly to the Commission and the Administration for Child Support Enforcement ("ASUME") the following information, which shall be deemed confidential:

a. A summary of cash winnings withheld for delinquent child support pursuant to the Regulations for Winning Wager Payment, which shall include, without limitation:
   i. The date on which the Operator withheld the cash winnings.
   ii. The amount of cash withheld for delinquent child support.
   iii. The amount of cash retained for an administrative fee in the amount of the lesser of one hundred dollars ($100) or three percent (3%) of the amount of delinquent child support withheld
   iv. The following information from the obligor:
      1) Full name.
      2) Address.
      3) Last four (4) digits of the obligor's Social Security number.
      4) The child support case identifier for the case to which ASUME will apply the withheld cash winnings.
      5) The name of the person who prepared the summary.

b. An updated list of the names of the employees who are authorized to participate in the withholding process.

9.7.3 Redemption During System Failure

The Operator shall submit to the Commission, for its approval, manual procedures that will be followed during times of system failure.

a. In the event of a failure of the Sports Betting System's ability to pay winning wagers, the Operator shall have internal controls detailing the method of paying these wagers.

b. In case of Sports Betting System failure, winning wager tickets/vouchers may be paid. For all payouts, including payouts for contest/tournament winners, that are made without Sports Betting System authorization (i.e., system inoperative):
   i. After the manual grading of the winning wager ticket/voucher, the date and time must be stamped on the player's copy, and the amount of the payment and a paid designation is written (or stamped) on the player's copy of the winning wager ticket/voucher by the employee;
   ii. Before completing the payout, the Sports Betting Manager or other authorized supervisory personnel reviews the documentation supporting and explaining the payout and signs the wager ticket/voucher as evidence of review, and
   iii. An individual, once the Sports Betting System is operative, immediately enters all manually paid wager tickets/vouchers into the Sports Betting System to verify the accuracy of the amount paid for the wager tickets/vouchers and the manual grading of the wager tickets.

c. Any manually paid wager tickets that had been previously purged from the Sports Betting System do not need to be entered into the Sports Betting System.

9.7.4 Taxation Reporting

The Operator shall have a process in place to identify all wins that are subject to taxation (single wins or aggregate wins over a defined period as required) and prepare a W-2G before the winning player is paid, and withhold federal income tax as necessary, in compliance with IRS Rules. The Operator shall include in its submission, procedures

for the preparation and distribution of the W-2G which shall include, at a minimum, where and by whom the W-2G is prepared, how copies are distributed and how the win is adjusted, if necessary.

9.7.5 **Lost Wager Tickets and Vouchers**

The internal controls shall detail the procedures to redeem lost wager tickets or vouchers, which shall include a supervisor's approval and documentation of the:

a. The date and time of the redemption;
b. The employee responsible for redeeming the wager ticket or voucher;
c. The supervisor authorizing the redemption;
d. The name of the player redeeming the wager;
e. Unique wager ticket or voucher identifier; and
f. Location of the redemption.

9.7.6 **Payout Procedures for Mail-In Winning Wager Tickets and Vouchers**

Accounting Personnel or personnel independent of the Sports Betting Function receive the original winning wager tickets and vouchers.

a. Accounting Personnel or personnel independent of the Sports Betting Function record the winning wager tickets and vouchers on a log as a mail pay. The log includes the date received, player's name, and wager ticket numbers and voucher numbers.
b. The winning wager tickets and vouchers are entered into the Sports Betting System by Sports Betting personnel or Accounting Personnel for validation and cancellation.
c. Accounting Personnel compare the "paid" winning wager tickets and "paid" vouchers to the mail pay log and the Sports Betting System report for paid winning wager tickets and vouchers. Any discrepancies are documented and reviewed with sports betting and accounting management personnel.
d. Accounting personnel, independent of the individual(s) who processed the mail pay winning wager tickets and vouchers, reviews the player's correspondence submitted, the winning wager tickets and vouchers, the mail pay log and the Sports Betting System report for "paid" winning wager tickets and "paid" vouchers for any discrepancies. Any discrepancies are documented and resolved prior to remitting the proper payment amount to the player.

9.8 Layoff Wagers

9.8.1 The Operator may, in its discretion, accept a Layoff Wager placed by other Operators. Operators may place wagers only with other Operators. The Operator placing a Layoff Wager shall disclose its identity to the other licensed Operator accepting the wager.

9.8.2 The amounts of wagers placed by an Operator and the amounts received by the Operator as payments on such wagers shall not affect the computation of the Operator's Adjusted Gross Revenue.

9.8.3 Before an Operator accepts a wager from another Operator:

a. The authorized employee of the other Operator must personally appear at the Authorized Location of the Operator to open a Player Account;
b. The Operator employee must record:
    i. The authorized employee of the other Operator's name, permanent business address (other than a post office box number), and business telephone number;
    ii. The documents used to verify the other Operator is an Operator, the authorized employee is an employee of the other Operator and is authorized to open this Player Account;
    iii. The amount of the authorized employee of the other Operator's initial Player Account or front money deposit;
    iv. The authorized employee of the other Operator's account number with the Operator; and
    v. The date the authorized employee of the other Operator's account with the Operator is opened;
c. The authorized employee of the other Operator must sign, in the presence of a supervising employee of the Operator, statements attesting that the authorized employee of the other Operator:
    i. Confirms the accuracy of the information recorded;
    ii. Has received a copy, or has had a copy made available to them, of the Operator's rules and procedures for wagering communications;
    iii. Has been informed and understands that authorized employees of other Operators that establish a Player Account pursuant to these MICS are prohibited by law from placing wagering communications from outside the Commonwealth and that the Operator is prohibited by law from accepting them;

iv. Consents to the monitoring and recording by the Commission and the Operator of any wagering communication; and

d. The employee who verifies the authorized employee of the other Operator's information and who obtains and records the information on behalf of the Operator and the supervising employee described in subparagraph (c), must each sign statements that they witnessed the authorized employee's signature and confirmed the authorized employee of the other Operator's identity and residence.

Section 10.0 Contests/Tournaments, Bonuses and Promotions, and Player Loyalty Programs

10.1 Bonus or Promotional Payouts, Drawings and Giveaway Programs

10.1.1 The Operator may offer bonus or promotional payouts, and any other promotion including drawings and giveaway programs, provided the MICS within this section are met.

10.1.2 The rules and conditions for participating in bonus or promotional payouts, and any other promotion including drawings and giveaway programs are available to a registered player on the Mobile App or Site where the bonus or promotion is being conducted and are prominently displayed or available for player review at the Authorized Location.

10.1.3 When bonus or promotional payouts are associated with a Player Account the following requirements apply:

a. Bonus or promotional payouts initially appear as restricted player funds in the Player Account and may be used to wager as described in the specific rules for the particular bonus or promotion. For restricted player funds, delineate in the internal controls how such funds are identified within the Player Account and the order in which these are used for wagering;

b. Restricted player funds shall have no cash value and are not eligible for withdrawal. They must be played at least once in order to have the corresponding winnings available for withdrawal;

c. Winnings from restricted player funds must be able to be withdrawn without being subject to any further wagering requirements;

d. Bonus or promotional payouts are not transferable between Player Accounts;

e. The Operator shall provide a clear and conspicuous method for a player to cancel their participation in a bonus or promotion that utilizes restricted bonus or promotional payouts;

f. Upon request for cancellation, the Operator shall inform the player of the amount of unrestricted player funds that will be returned upon cancellation and the value of restricted player funds that will be removed from the Player Account;

g. If the player elects to proceed with cancellation, unrestricted player funds remaining in a Player Account shall be recounted in accordance with the conditions of the promotion or bonus.

h. Closure of the Player Account will render a promotion or bonus void; and

i. Once a player has met the conditions of the promotion or bonus, the Operator shall not limit winnings earned while participating in the offer (i.e., the restricted player funds will become unrestricted player funds).

10.1.4 The internal controls in respect of bonus or promotional payouts, including awards as a result of drawings and giveaway programs, and verification of same must include the following:

a. All bonus or promotional payouts and awards procedures, including verification controls.

b. The form or documentation completed in respect of bonus or promotional payouts and awards must include the following information:

i. The date and time;

ii. The amount of payout, or description and value of the prize awarded if not cash (e.g., jacket, toaster, car, etc.), including fair market value;

iii. The type of bonus or promotion;

iv. The reason for payout (e.g., bonus or promotion name);

v. Player's name and confirmation that identity was verified (drawings only); and

vi. Signature(s) of at least two employees verifying, authorizing, and completing the promotional payout with the player. For systems that validate and print the dollar amount of the payout on a computer-generated form, only one employee signature is required on the payout form.

c. The documentation of (b) may be prepared by an individual who is not Sports Betting Personnel as long as the required signatures are those of the employees completing the payout with the player.

10.2 Player Loyalty Programs

10.2.1 The MICS within this section apply to player loyalty programs where players accumulate points, typically based on the volume of wagering or revenue received from a player, that are subsequently redeemed by the player for wagering credits, cash, merchandise, etc.

10.2.2 Rules and policies for the player loyalty program including the awarding, redeeming and expiration of points are available to a registered player on the Mobile App or Site and prominently displayed or available for player review at the Authorized Location where the player loyalty program activity is being conducted.

10.2.3 Player loyalty information shall be stored in a database that permits ad hoc inquiry and reporting activities in addition to routine, scheduled reporting.

10.2.4 The addition/deletion of player loyalty points other than through an automated process related to actual wagering must be sufficiently recorded (including substantiation of reasons for increases) and authorized/performed by appropriate supervisory personnel. This MICS does not apply to the deletion of points related to dormant and closed accounts through an automated process.

10.2.5 The Operator shall remove excluded persons from player loyalty programs.

10.2.6 Employees who redeem points for players cannot have access to dormant and closed accounts without supervisory personnel authorization. Documentation of such access and approval is created and maintained.

10.2.7 Player identification is required when redeeming points without a player loyalty card.

10.2.8 Changes to the player loyalty parameters, such as point structures and employee access, must be performed by supervisory personnel independent of the Sports Betting Function. Alternatively, changes to player loyalty account parameters may be performed by the Sports Betting Manager if sufficient documentation is generated and the propriety of the changes is randomly verified by personnel independent of the Sports Betting Function on a quarterly basis.

10.2.9 All other changes to the player loyalty program must be appropriately documented.

10.3 Complimentary Services or Items

10.3.1 Each Operator shall establish and include in its approved internal controls, procedures for the authorization, issuance, recording and monitoring of complimentary services or items, including cash and non-cash gifts. Such procedures shall include all system controls and detail, at a minimum, the following:

a. The procedures by which the Operator delegates to its employees the authority to approve the issuance of complimentary services or items, including levels of authorization
b. The limits and conditions on the approval and issuance of complimentary services or items, if any, which may apply to such authority are established and modified (including limits based on relationships between the authorizer and recipient); and
c. Making and documenting changes to conditions or limits on the approval and issuance of complimentary services or items
d. Documenting and recording the authorization, issuance, and redemption of complimentary services or items, including cash and non-cash gifts;
e. Effective provisions for audit purposes.

10.3.2 At least monthly, accounting, IT, or audit personnel that cannot grant or receive complimentary privileges shall prepare reports that include the following information for all complimentary items and services equal to or exceeding $100 or an amount established by the Operator and approved by the Commission, which shall not be greater than $100:

a. Name of player who received the complimentary service or item;
b. Name(s) of issuer(s) of the complimentary service or item;
c. The actual cash value of the complimentary service or item;
d. The type of complimentary service or item (i.e., food, beverage); and
e. The date the complimentary service or item was issued.

10.3.3 The Internal Audit or Accounting Function shall review the reports at least monthly. These reports shall be made available to the Commission, audit committee, or other entity designated by the Commission upon request.

10.3.4 Complimentary services and items records must be summarized and reviewed for proper authorization and compliance with established authorization thresholds.

10.3.5 A detailed reporting of complimentary services or items transactions that meet an established threshold approved by the Commission must be prepared at least monthly.

10.3.6 The detailed report must be forwarded to management for review.

10.3.7 The report must be made available to those entities authorized by the Commission or by Commonwealth law or ordinance.

10.4 Contests and Tournaments

10.4.1 A contest/tournament, which permits a player to either purchase or be awarded the opportunity to engage in competitive wagering against other players, may be conducted by Operators, provided the MICS within this section are met.

10.4.2 Contest/tournament rules are available to a registered player on the Mobile App or Site where the contest/tournament is being conducted, included on all entry forms/brochures, and are prominently displayed or available for player review at the Authorized Location.

10.4.3 A player is to register prior to being allowed to participate in a contest/tournament and the player is to provide the following information:

a. Player's name;
b. Player's date of birth; and
c. E-mail address.

10.4.4 Procedures are to be performed to verify that:

a. A player registering to participate in a contest/tournament is 18 years of age or older.
b. Contest/tournament awards are paid to a registered player who is 18 years of age or older.

10.4.5 When contest/tournament entry fees and payouts are transacted, the transactions are recorded on a document which contains:

a. Player's name.
b. The date of entry/payout.
c. Amount of entry fee/payout (both alpha and numeric, or unalterable numeric) and/or nature and dollar value of any non-cash payout.
d. Signature of individual completing transaction attesting to the receipt or disbursement of the entry fee/payout with the player and, for contest/tournament winners, the verification through the Sports Betting System of the winner.
e. Name of contest/tournament.

10.4.6 Operators shall include in their internal controls the procedures to be used to document and account for all funds collected and distributed for contests and tournaments.

10.4.7 The contest/tournament entry fees and payouts are summarized and posted to the accounting records on at least a monthly basis. It is acceptable to post on a monthly basis to the general ledger, one entry, in total, for contest/tournament entry fees and payouts.

10.4.8 For one day each week, two employees, one of whom is independent of the collection of entry fees, will randomly select two contests/tournaments and reconcile the total amount of issuance for the contest/tournament in exchange for entry fees to the final amount at the end of the contest/tournament. The reconciliation is documented and signed by the employees.

10.4.9 The results of each contest/tournament, held during the prior two operational days, are recorded and available on the Mobile App or Site for the participants to review and are prominently displayed or available for participants review at the Authorized Location. The name of each winner is also recorded and maintained but not made available to the participants unless authorized by management personnel.

Section 11.0 Sports Betting Risks and Controls

11.1 Events, Odds and Result Management

11.1.1 Procedures regarding the selection of the Sports Events or Special Events and for setting and updating the odds/payouts and prices and/or blocking events as well as for receiving the results from reliable sources shall be established within the internal controls. A process shall exist for validating accuracy and preventing fraudulent activities. The procedures shall be based on the respect of integrity, player protection, and ensuring transparency and involve several levels of authority. Logs and other audit trails must exist to prevent possible misuse of authority.

11.1.2 The Operator must establish a set of measures in the internal controls to ensure authorized payout levels are not exceeded.

11.1.3 The results for a Sports Event or Special Event become the official results when the Operator enters the results in the Sports Betting System. Before the results are finalized, the Operator may recognize changes to the results and resettle wagers, but once the results are finalized, the Operator will generally not recognize changes including, but not

limited to, the game's final score, or any protests, overturned decisions, or statistical changes made by the Sports Governing Body or equivalent that changes the final score or call on a particular play.

11.1.4 The internal controls shall delineate how errors involved with wagers and a resettlement of the wager may be handled. Errors for purposes of resettlement include, operator errors, the Sports Governing Body or equivalent changes a call on a particular play or final score or a malfunction may cause winnings to be incorrectly credited to the Player Account.

11.2 Monitoring Activities and Reporting Fraud and Suspicious Conduct

11.2.1 Procedures shall be established to monitor all changes to odds/payouts and prices and/or blocking throughout a Sports Event or Special Event, monitoring of the events and player transactions for the detection of irregularities, monitoring of winners over a certain amount of gains, and deposits over a certain size. The procedures shall also specify thresholds of payment and methods of collection.

11.2.2 The internal controls shall delineate how the Operator reserves the right to suspend the Player Accounts involved in any possible syndicates or if it appears that a series of wagers contain duplicative or identical selections made by, or on behalf of, the same person or group of people, or in their favor, until an investigation is completed. These winnings are ineligible for payment until an investigation is completed.

11.2.3 The Operator shall have internal controls and monitoring in place to identify Unusual and Suspicious Activity and report such activity in accordance to the Operator's Integrity Monitoring Procedures approved by the Commission.

a. The Operator's Integrity Monitoring Procedures shall provide for sharing copies of information with each Operator, as necessary, and include the requirement that the Operator shall disseminate all reports of Unusual and Suspicious activity to the Commission. Operators are encouraged to share information with other Operators, and coordinate with an approved independent integrity monitoring provider to determine whether other Operators have experienced similar activity in the Commonwealth or any other jurisdiction where operating. All Unusual Activities are to be reported to the Commission immediately.

b. If the Operator finds that previously reported Unusual Activity rises to the level of Suspicious Activity or if an activity constitutes Suspicious Activity, it shall immediately notify the Commission. Examples of the monitoring and reporting requirements for unusual and suspicious activity at a minimum include:

   i. Attempts to violate or evade any local or federal law or regulations pertaining to Sports Betting in any jurisdictions;
   ii. Violations or attempted violations of local or federal Anti-Money Laundering (AML) laws;
   iii. Unusual or suspicious behavior or patterns of Wagers by Player as determined by the Operator;
   iv. Unusual geographical concentration betting;
   v. Wagers that have been placed online or through a mobile device using different accounts but having the same IP address;
   vi. Unusual and abnormal proportion of bets against the favorite or for the underdog; or
   vii. Unusual volumes of betting relative to the norm.

c. The Operator must also submit an annual report to the Commission which details its integrity monitoring services and activities and summarizes all Suspicious Activity notifications issued during the year.

d. The Operator with knowledge or reasonable suspicion of Suspicious Activity shall be permitted to suspend wagering on related events but may only cancel or rescind related wagers after receiving Commission approval.

e. The information provided to the Commission 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 or equivalent within the sole and absolute discretion of the Commission.

f. The Operator shall provide remote access and the necessary hardware for the Commission to evaluate its Sports Betting Operations or for the Commission to conduct further monitoring of the Sports Betting System.

11.3 Global Risk Management

11.3.1 The Commission shall be provided with information regarding an intent by the Operator to utilize Global Risk Management, including a copy of the written agreement for those services. The Commission may reject the use of such services for any reason deemed reasonable in the preservation of the integrity of the Law and Regulations.

11.3.2 The following are permissible services which an Operator or Service Provider licensed by a regulatory authority in another permissible jurisdiction may perform in the Commonwealth:

a. Setting, modifying, or providing risk management advice as it relates to odds, point spreads, and lines;

b. Deciding when a Sports Event or Special Event should be removed as an option from the list of Sports

Events and Special Events authorized by the Commission and offered by the Operator;

c. Determining when the wagers by Players on a particular Sports Event or Special Event should be rejected;
d. Determining when it would be desirable to place Layoff Wagers with another licensed Operator in the Commonwealth; or
e. Using their special expertise to manage the risks associated with Sports Betting in the Commonwealth.

11.3.3 An Operator or Service Provider engaging in global risk management may provide direction, management, consultation, and/or instruction to another Operator located in a permissible jurisdiction concerning:

a. The management of risks associated with sports betting involving a Sports Event or Special Event for which a wager may be accepted;
b. The determination of where lines, point spreads, odds, or other activity relating to sports betting are initially set and the determination of whether to change such lines, point spreads, odds, or other activity relating to wagering;
c. Whether or not to accept or reject wagers, to pool wagers, or to lay off wagers;
d. The use, transmittal, and accumulation of information and data for the purpose of providing global risk management; and
e. Any other activity associated with Sports Betting if approved in writing by the Commission prior to an Operator or Service Provider commencing direction, management, consultation, and/or instruction concerning the activity.

11.3.4 The Operator or Service Provider which intends to provide global risk management shall:

a. Enter into a written agreement to provide global risk management with another Operator to which the Operator or Service Provider proposes to provide global risk management. A copy of such executed agreement with the other Operator shall be provided to the Commission no later than the date on which the Operator commences global risk management for the other Operator;
b. Provide details to the Commission regarding any permissible jurisdiction other than the Commonwealth where the Operator or Service Provider intends to provide global risk management no later than the date on which the Operator commences global risk management in such permissible jurisdiction;
c. No later than the date on which an Operator or Service Provider commences global risk management, submit the internal controls utilized by the Operator or Service Provider for global risk management to the Commission. Such internal controls must include provisions for complying with all federal laws and regulations; and
d. Provide such other information as the Commission may require concerning global risk management.

11.3.5 In addition to these MICS, at least 30 days prior to providing global risk management to another licensed Operator in the Commonwealth, an Operator shall submit to the Commission the written agreement for the global risk management provided to the other licensed Operator in the Commonwealth. The Commission may object in writing to such agreements in the Commission's sole and absolute discretion. If the Commission objects to an agreement, the Operator shall not provide global risk management to the other licensed Operator in the Commonwealth until the Operator has resubmitted the agreement to the Commission, and the Commission has indicated in writing that the Commission does not object to the resubmitted agreement.

11.4 Location Service Providers

The Operator or a third-party Location Service Provider (LSP) used to provide location-based services and the border control technology for the identification of and the geographic location of players as authorized by the Commission shall undergo a specific annual audit, where required by the Commission. Internal controls shall delineate how:

a. Information relating to confirming a player's location and the location of their computer or Mobile Device may be shared with Operator or LSP contractors, sub-contractors, affiliates and other third-parties for a variety of reasons, including but not limited to: providing the product, service or transaction the player requested, legal compliance purposes, and marketing purposes.
b. The Operator or LSP facilitates routine, recurrent delivery of supplemental fraud reports pertaining to suspicious or unusual activities, account sharing, malicious players and devices, as well as other high-risk transactional data.
c. The border control technology used for location detection:
    i. Utilizes closed-source databases (IP, proxy, VPN, etc.) that are updated daily and periodically tested for accuracy and reliability; and
    ii. Undergoes frequent updates, at least once every ninety (90) days, to maintain cutting-edge data collection, device compatibility, and fraud prevention capabilities against location fraud risks,

including, remote desktop software, rootkits, virtualization, or any other programs identified by the Commission having the ability to circumvent location-based services.

d. The Commission is provided evidence, at least every ninety (90) days, that the border control technology is updated to the latest solution.

Section 12.0 Authorized Location

12.1. **Hours of Operation**

12.1.1. The Authorized Location may only operate according to the hours approved by the Commission. The Operator will present the Commission with a proposed schedule and will obtain the approval of said schedule before implementing it. All schedule changes will be presented and approved by the Commission before being implemented.

12.1.2. During authorized hours, the Operator will assign the number of licensed employees required by the Commission in each shift to attend and maintain the Kiosks and Ticket Writer Stations and authorize and facilitate wagers and the payments of the winnings.

12.1.3. If an Authorized Location has to shut down due to unforeseen circumstances and the closure is unscheduled, the Commission shall be informed immediately.

12.2. **Betting Counters and Windows**

12.2.1. Each Authorized Location shall include betting counters and windows that shall:

a. Be designed and constructed to provide maximum security for the materials stored and the activities performed therein;

b. Include one or more betting windows, each of which shall contain:

i. A cashier's drawer and Ticket Writer Station through which financial transactions related to sports betting are conducted;

ii. A physical barrier designed to prevent direct access to the materials stored and activities performed at such betting counter. and

c. If required by the Commission, include manually triggered silent alarm systems, which shall be connected directly to the surveillance monitoring room;

d. If required by the Commission, have an alarm for each emergency exit door that is not a mantrap; and

e. Include a secure location for the purpose of storing funds issued by a cage to be used in the operation of sports betting.

12.2.2. Temporary betting counters are accepted so long as they meet the following:

a. When temporary betting counters are in use:

i. Physical barriers are to be installed to prevent unauthorized individuals (e.g., members of the public) from direct access to area containing the Ticket Writer Station and safe;

ii. Physical security will be available to prevent unauthorized individuals from direct access to the area containing the Ticket Writer Station and safe; and

iii. Surveillance cameras shall provide coverage of individuals placing wager and individuals accepting wager.

b. When temporary betting counters are not in use:

i. All financial instruments shall be removed from the cash register/safe and Ticket Writer Stations shall be locked to prevent unauthorized access;

ii. Surveillance camera requirements noted above must remain in place irrespective of the betting counters being moved to different locations; and

iii. Surveillance cameras shall continue to monitor the area and will be supplemented by physical security personnel, as needed;

c. A sign will be displayed informing the public when temporary betting counters are closed.

12.3. **Main Cage**

12.3.1. **Computer Applications**

For any computer applications utilized, alternate documentation and/or procedures that provide at least the level of control described by the MICS in this section, as approved by the Commission shall be acceptable.

12.3.2. **Account Controls for a Main Cage**

To conduct sports betting**,** an Authorized Location shall have a main cage that has been approved for the operation by the Commission.

a. Operators may only conduct transactions with individuals at its main cage, betting counter, betting window, and any satellite cage (collectively referred as main cage) during the hours of operation approved by the Commission.

b. Each betting window and counter shall have a dedicated cash register/safe for the storage of financial instruments. The movement or physical transfer of financial instruments shall be restricted to the count staff and/or security. Records and documentation of deposits and withdraws from cash register/safe shall be maintained and are to include the names of individuals performing said function including dollar amounts of financial instruments, date and time of transactions.

c. A cage supervisor or equivalent must be available at all times during the time sports betting is taking place. Ticket Writers (i.e., Individuals accepting wagers and making payouts) must have a valid, unexpired, occupational license issued by the Commission.

d. The Operator shall:
   i. Provide ticket writers with instructions regarding payouts, winning wager ticket and voucher validation, winning wager ticket and voucher handling and storage, reporting of security issues, and the handling of lost and stolen wager tickets and vouchers;
   ii. Implement procedures to ensure the validity of winning wager tickets and vouchers;
   iii. Establish a process for payment or transfer of winnings;
   iv. Maintain in its main cage a reserve bankroll sufficient to pay all winning wagers;
   v. Compute its reserve cash bankroll requirement each day; and
   vi. Submit its computation to the Commission:
      1) At least 30 days prior to the commencement of sports betting operations;
      2) Within 24 hours in the event the Operator determines that their reserve is not sufficient to cover the calculated requirement; and
      3) Annually in which a license is issued.

e. The Ticket Writer Station shall be secured through password, biometrics or other similar means. Generic passwords for the Sports Betting System are prohibited for cashiers unless:
   i. Each ticket writer redeems wager tickets and vouchers from the ticket writer's assigned window.
   ii. After verifying the winning wager ticket or voucher in the Sports Betting System, the cashier then signs the player's copy of the wager ticket, immediately date/time stamps the wager ticket or voucher at the cashier's assigned window, and then maintains the wager ticket or voucher in the cashier's cash drawer.
   iii. Each ticket writer is assigned a unique date/time stamp used solely at the ticket writer's assigned window.
   iv. Payouts of $3,000 or more require the supervisor to enter the supervisor's approval code and to sign the wager ticket.
   v. Payouts exceeding any Tax Reporting Thresholds require the supervisor to enter the supervisor's approval code and to sign the wager ticket. In addition, the provisions of MICS 10.5.4 shall be met.
   vi. Deposits, withdrawals, or payouts of $10,000 or more require supervisory personnel to enter an approval code and to sign the wager ticket or voucher (as applicable). In addition, the provisions of MICS 15.2 shall be met.
   vii. A summary sheet is prepared which lists all of the cashiers working that shift, the cashiers' assigned windows, the date/time stamp identification, and the total wager tickets cashed per cashier. The total of that report is then balanced to the total cashed per the Operator end-of-shift report.
   viii. Any discrepancies noted and investigations performed are documented in writing and maintained.

f. The previous MICS does not apply when a supervisor signs onto a common terminal with his or her individual password and the supervisor takes responsibility for the sports betting payouts.

g. The internal controls shall detail procedures to reprint tickets/vouchers that fail to print at either a Ticket Writer Station or Kiosk. Such procedures shall include a requirement of supervisory authorization for the reprint

h. The Operator shall provide the Commission with the start and end time of each cage shift. The times shall not be changed without prior Commission approval.

12.3.3. **Employee Segregation of Duties**

The Operator shall develop and include in the internal controls addressing the segregation of the main cage, and the general conduct of the main cage transactions.

a. Ticket writers shall be responsible for:
   i. An individual imprest inventory of cash;
   ii. Receipt and payout of cash, negotiable instruments, vouchers, and other records from and to players subject to limitation imposed under these MICS;
   iii. Preparation of wager ticket records; and

iv. Other functions designated by the Operator which are not incompatible with the functions of a ticket writer.

b. Main bank cashiers or other approved by the Commission shall be responsible for:
   i. Receipt of cash, negotiable instruments, vouchers, and other records from ticket writers in exchange for cash or documentation;
   ii. Receipt of unsecured cash and unsecured vouchers;
   iii. Receipt of cash and documentation from the count room etc.;
   iv. Preparation of the overall main cage reconciliation;
   v. Preparation of bank deposits;
   vi. Compliance with reserve bank roll requirements;
   vii. Receipt of original and redemption copies of counter checks;
   viii. Receipt from ticket writers of documentation supporting counter check substitution, consolidation, or redemption; and
   ix. Other functions designated by the Operator which are not incompatible with the functions of a main bank cashier.

c. Employees who perform the supervisory function of approving wager ticket voids do not write wager tickets unless:
   i. The only supervisory function allowed is approval of wager ticket voids prior to post time;
   ii. A supervisor, acting as a writer, may not authorize a void for a wager ticket which he wrote;
   iii. All wager tickets written by a supervisor which are subsequently voided and all not-in-computer voids must be recorded in a log, used specifically for that purpose, which indicates the supervisor's/writer's name, occupational license number, and the name of the person (including occupational license number) authorizing the void;
   iv. The log must be forwarded to a function independent of the Sports Betting Function (i.e., Accounting Function) on a daily basis for a 100% audit of void wager tickets (using the log and the wager tickets) for the proper signatures (includes occupational license number) on the wager ticket, a void designation on the wager ticket, date and time of the void on the wager ticket (for not-in-computer voids), any indications of past-post voiding, and other appropriate regulation compliance. Any discrepancies noted and investigations performed must be documented in writing and maintained;
   v. A function independent of the Sports Betting Function (i.e., Accounting Function) must perform a 100% audit of the exception report for any inappropriate use of the supervisory password. Any discrepancies noted and investigations performed must be documented in writing and maintained.

d. Employees, including supervisors, who write or cash wager tickets are prohibited from accessing the administrative terminal or performing administrative functions, including setting up events, changing event data, and entering results at any time. An employee assigned cashier functions is not allowed to switch for certain shifts or days to having administrative functions. Conversely, an employee assigned administrative functions is not allowed to switch for certain shifts or days to having cashier functions.

e. The Operator shall prohibit an employee or employee who is serving alcoholic beverages to customers from taking sports wagers during the same work shift.

f. Employees authorized to destroy redeemed winning wager tickets and vouchers shall be formally defined. The method and control of redeemed winning wager ticket and voucher destruction shall be established.

12.3.4. **Cage Access**

Internal controls must be established, and procedures implemented to:

a. Restrict physical access to the cage to only cage employees, designated staff, and other authorized persons; and

b. Limit transportation of extraneous items such as personal belongings, toolboxes, beverage containers, etc., into and out of the cage.

12.3.5. **Cage Accountability**

All cage accounting procedures and any follow-up performed shall be documented in the internal controls, maintained for inspection and provided to the Commission upon request.

a. The Operator shall establish policies and procedures to ensure that all transactions that flow through the main cage within the Authorized Location are accounted for. These policies and procedures shall include, but are not limited to, the following:
   i. All transactions that flow through the cage shall be summarized on a cage accountability form on a per shift basis and shall be supported by documentation;

ii. Increases and decreases to the total cage inventory must be verified, supported by documentation, and recorded. Documentation must include the date and shift, the purpose of the increase/decrease, the employee(s) completing the transaction, and the person or function receiving the cage funds (for decreases only);

iii. At the end of a shift, the ticket writers assigned to the outgoing shift shall:

1) Record on a cage accountability form, or its equivalent, the face value of each cage inventory item counted and the total of the opening and closing cage inventories;

2) Reconcile the total closing inventory with the total opening inventory;

iv. At the conclusion of each operational day, copies of the cage accountability forms and all supporting documentation shall be forwarded to the Accounting Function; and

v. Signature requirements shall be established for outgoing and incoming ticket writers.

b. The cage inventories shall be counted independently by the oncoming and outgoing ticket writers. These employees shall make individual counts for comparison for accuracy and maintenance of individual accountability. Such counts shall be attested to by signature and recorded at the end of each shift during which activity took place. These employees must make individual counts to compare for accuracy and maintain individual accountability. All variances of more than **$500.00** must be documented and investigated. Unverified transfers of financial instruments are prohibited.

c. The Operator shall establish and comply with procedures with a minimum bankroll formula to ensure the Operator maintains financial instruments (on hand and in the bank, if readily accessible) in an amount sufficient to satisfy obligations to the Operator's players as they are incurred.

12.3.6. **Ticket Writer Station Reconciliation of Assets and Documents**

The assets for which each Ticket Writer is responsible for shall be maintained on an imprest basis. A Ticket Writer shall not permit any other person to access his or her imprest inventory.

a. A Ticket Writer shall begin a shift with an imprest amount of financial instruments to be known as the "Sports Betting Inventory." The Main Bank shall provide the Sports Betting inventory to ticket writers for Sports Betting. No funds shall be added to or removed from the Sports Betting inventory during such shift except:

i. In collection of wagers;

ii. In order to make change for a player buying a wager ticket;

iii. In payment of winning or properly cancelled or refunded wager tickets;

iv. In payment for vouchers; or

v. In exchanges with the main cage, a satellite cage, or betting counter supported by proper documentation which documentation shall be sufficient for accounting reconciliation purposes.

b. Whenever a ticket writer exchanges funds with the Main Bank, the ticket writer shall prepare a two part Even Exchange form. The form shall include at a minimum the following:

i. The date of preparation;

ii. Window location;

iii. Separate areas designating which items are being sent to/received from the Main Bank;

iv. The type of items exchanged;

v. The total of the items being exchanged;

vi. Signature of the ticket writer preparing the form requesting the exchange; and

vii. Signature of the main bank cashier completing the exchange.

c. Each ticket writer and main bank cashier shall prepare a "Sports Betting Count Sheet" on each shift, including

i. Recording the amount of inventory in the betting window or bank; and

ii. Reconciling the total closing inventory with the total opening inventory;

iii. Recording the signature and employee occupational license number of the:

1) Outgoing ticket writer or main bank cashier; and

2) Incoming ticket writer or main bank cashier;

iv. Recording the following information:

1) The date, time and shift of preparation;

2) The total amount of each denomination of currency in the drawer;

3) The total of any exchanges;

4) The total amount in the drawer;

5) The value of the sold, voided, and cashed wager tickets or attach a printout from the system to the count sheet

6) The total amount of financial instruments in the Sports Betting inventory issued to the Ticket Writer;

7) The betting window number to which the Ticket Writer is assigned; and

8) If the cash is transferred from one Ticket Writer to the next Ticket Writer, the amount of cash turn-in and any variances between the cash turn-in and the amount of net cash that the Sports Betting System indicates must be in each Ticket Writer Station.

d. A Ticket Writer assigned to a betting window shall count and verify the Sports Betting inventory at the count room and shall agree the count to the "Sports Betting Count Sheet". The Sports Betting inventory shall be placed in a ticket writer's drawer and transported directly to the Ticket Writer Station by the Ticket Writer.

e. At the end of the operational day, the main cage is to forward a copy of each ticket writer's "Sports Betting Count Sheet" and related documentation to the Accounting Function for:
   1) Agreement of opening and closing inventories; and
   2) Comparison of forms or documents.

f. If the betting window net receipts for the shift, as generated by the system, does not agree with the Sports Betting Count Sheet total plus the Sports Betting inventory, the shift supervisor shall record any overage or shortage on a Ticket Writer Variance log. If the count does not agree, the ticket writer and the shift supervisor shall attempt to determine the cause of the discrepancy in the count. If the discrepancy cannot be resolved by the Ticket Writer and the shift supervisor, such discrepancy shall be reported in writing to the Sports Betting Manager, or supervisor in charge at such time and documentation will be provided to the Accounting Function. Any discrepancy in excess of **$500.00** shall be reported to the Surveillance function and the Commission within two hours of the supervisor's shift ending, utilizing the Commission's incident report form.

g. The shift supervisor shall compare the betting window net receipts for the shift as generated by the system with the Sports Betting Count Sheet total plus the Sports Betting inventory, and if the ticket writer net receipts equals the wagering count sheet total plus the wagering inventory, the shift supervisor shall sign the Sports Betting Count Sheet attesting to its accuracy.

h. The Operator shall determine the daily win amount by comparing the Win Summary Reports from the Sports Betting System to the reconciliation of the sports betting drawers. The Operator shall be required to report sports betting revenue as the higher amount unless otherwise authorized by the Commission.

12.4. Kiosks

12.4.1. Kiosks Identification

Every Kiosk shall have the following identification characteristics:

a. Certificate of license issued by the Commission; and

b. A permanent printed label stamped and visibly affixed to the upper left of the kiosk cabinet display. It will be assigned and set by the Commission to each approved Kiosk. The following are characteristics of the label:
   i. It will display a unique identification number;
   ii. It will refer to the number of the inspection certificate; and
   iii. It will be assigned to a specific kiosk and cannot be removed or transferred for use in another Kiosk.

12.4.2. Access to Kiosks

The internal controls in respect of access to Kiosks must include, but not be limited to, the following:

a. Control measures to ensure that only authorized, registered employees of the Operator, registered employees on an Authorized Location, and a Commission licensed Supplier, may access the secure area of a Kiosk.

b. The requirement that all doors of the Kiosks are secured at all times.

c. The requirement of recording of relevant entries in a log each time a Kiosk is accessed (MEAL).

12.4.3. Kiosk Cash Storage Box

Each cash storage box used with a kiosk shall have an asset number permanently imprinted, affixed or impressed on its outside, which is sufficient in size to be clearly visible and readable by the CCTV System. This number should correspond to the asset number of the Kiosk to which the bill validator has been attached, except that emergency cash storage boxes may be maintained without such number, provided the word "emergency" is permanently imprinted, affixed, or impressed thereon, and when put into use, are temporarily marked with the asset number of the Kiosk to which the bill validator is attached.

12.4.4. Collecting Currency Cassettes and Cash Storage Boxes from Kiosks

Internal controls must be established, and procedures implemented to ensure that currency cassettes and cash storage boxes are securely removed from Kiosks on a daily basis, unless otherwise agreed to by the Commission.

a. Surveillance personnel must be notified prior to the cash storage boxes or currency cassettes being accessed in a Kiosk. The drop shall be monitored and recorded by surveillance.

b. The Operator shall submit the drop schedule to the Commission, which shall include

i. The time the drop is scheduled to commence; and
ii. The number and locations of Kiosks

c. At least two employees must be involved in the collection of currency cassettes and/or cash storage boxes from Kiosks and at least one employee should be independent of Kiosk accountability.

d. Currency cassettes and cash storage boxes must be secured in a manner that restricts access to only authorized employees.

e. Redeemed vouchers and winning wager tickets (if applicable) collected from the Kiosk must be secured and delivered to the Cage or Accounting for reconciliation.

f. A Security Function member and a Main Cage Function member shall obtain the keys necessary to perform the drop and/or currency cassette replacement, in accordance with the Authorized Location's key sign-out and sign-in procedures.

g. A function member with no incompatible functions shall place empty cash storage boxes needed for the drop into a secured cart and prepare a drop form, which shall include the following:
   i. The date;
   ii. Identification number of the secured cart;
   iii. Number of empty cash storage boxes placed into the secured cart; and
   iv. Signature of the Main Cage Function member documenting that the number of cash storage boxes equals the number of Kiosks in use.

h. In the presence of a Security function member, a Main Cage Function member shall complete the drop at each Kiosk by:
   i. Unlocking the cabinet housing the cash storage boxes;
   ii. Removing the cash storage boxes and place the removed cash storage boxes into a secured cart and insert the empty cash storage boxes and reject bins;
   iii. Locking the cabinets housing the cash storage boxes; and
   iv. Transporting the secured cart to a count room or other location approved by the Commission for the count of the drop.

12.4.5. **Kiosk Count and Documentation**

Kiosks must be maintained on the cage accountability and must be counted independently by at least two employees, documented, and reconciled for each increase or decrease to the Kiosk inventory.

a. Access to stored full cash storage boxes and currency cassettes must be restricted to:
   i. Authorized employees; and
   ii. In an emergency, authorized persons for the resolution of a problem.

b. The Kiosk count must be performed in a secure area, such as the cage or count room.

c. If counts from various revenue centers and Kiosks occur simultaneously in the count room, procedures must be in effect that prevent the commingling of funds from the Kiosks with any revenue centers.

d. The cash storage boxes and currency cassettes must be individually emptied and counted so as to prevent the commingling of funds between Kiosks until the count of the Kiosk contents has been recorded. At least daily, all winning wager tickets and vouchers in the Kiosk are removed by a minimum of two employees.

e. The contents of the cash storage boxes shall be counted by two or more Accounting Personnel with no incompatible function, who shall:
   i. Document the contents, by item and amount, for each cash storage box on a balance receipt;
   ii. Prepare or generate a drop totals report that summarizes the total currency, wager tickets, and vouchers counted;
   iii. Verify that the number of cash storage boxes counted equals the number of empty cash storage boxes initially recorded on the drop form. Any exceptions encountered during the drop and count process shall be documented on this form;
   iv. Transfer the currency to a main bank cashier with a copy of the drop totals report;
   v. Transport the wager tickets and vouchers to a secured location approved by the Commission for storage until permitted to destroy; and
   vi. Transport the balance receipts, the drop totals report and drop form to the Accounting Function.

f. The contents of each removed currency cassette and currency cassette reject bin shall be counted by two or more Accounting Personnel with no incompatible function, who shall:
   i. Document the count of each currency cassette and reject bin on a balance receipt, by Kiosk;
   ii. Prepare or generate a currency cassette replenishment totals report that summarizes the total currency counted;
   iii. Transfer the currency to a main bank cashier with a copy of the currency cassette replenishment totals report; and

iv. Transport the balance receipts and currency cassette replenishment totals report to the Accounting Function.

g. Procedures must be implemented to ensure that any corrections to the count documentation are permanent, identifiable, and the original, corrected information remains legible. Corrections must be verified by two employees.

12.4.6. **Kiosk Replenishment**

Currency cassettes must be secured with a lock or tamper resistant seal and, if not placed inside a Kiosk, must be stored in a secured area of the cage or count room.

a. On a daily basis or at a greater frequency as needed, an Operator shall replenish the currency cassettes in the Kiosks. A cashier with no incompatible functions shall prepare the currency cassettes to replenish the Kiosks, which shall be documented on a two-part cassette fill form. The cashier shall retain one copy of such form and the duplicate shall be used to document the completion of the transaction. The form shall include:
   i. Designation of the Kiosk to which the fill is to be performed;
   ii. For each denomination, the number of bills and total value;
   iii. The total value of all currency cassettes;
   iv. The date and time prepared; and
   v. Signature of the cashier.

b. Accounting Personnel shall place the replacement currency cassettes and empty reject bins into a secured cart. In the presence of a Security function member, the Accounting Personnel shall complete the currency cassette replenishment at each Kiosk.

c. Internal controls must be established, and procedures implemented to ensure that currency cassettes contain the correct denominations and have been properly installed.

12.4.7. **Kiosk Reconciliation of Assets and Documents**

Whenever employees remove winning wager tickets or vouchers from a Kiosk, or cash is removed from or inserted into a Kiosk, reports are generated regarding transactions and accountability. These reports are compared to the transactions recorded by the Sports Betting System, if separate.

a. The Accounting Function shall reconcile the Kiosks on a daily basis and whenever employees remove winning wager tickets, vouchers or cash from a Kiosk pursuant to internal controls as follows: all the cash remaining in each Kiosk (including cash accepted by the Kiosk) to the cash initially loaded into the Kiosk (i.e., imprest amount) plus/minus cash transactions.

b. Any variance of **$500.00** or more shall be documented by the Accounting Function and reported in writing to the Commission within 72 hours of the end of the operational day during which the variance was discovered. The report shall indicate the cause of the variance and shall contain any documentation required to support the stated explanation. Such procedures shall be detailed in the internal controls approved by the Commission.

c. Winning wager tickets and vouchers are ultimately delivered to the Accounting Function.

12.5. **Count Room Access and Count Team**

12.5.1. Internal controls must be established, and procedures implemented to limit physical access to the count room to count team employees, designated staff, and other authorized persons. Such internal controls must include the following:

a. Count team employees may not exit or enter the count room during the count except for emergencies or scheduled breaks;

b. Surveillance personnel must be notified whenever count room employees exit or enter the count room during the count; and

c. The count team policy, at a minimum, must address the transportation of extraneous items such as personal belongings, toolboxes, beverage containers, etc., into or out of the count room.

12.5.2. Internal controls must be established, and procedures implemented to ensure security of the count and the count room to prevent unauthorized access, misappropriation of funds, forgery, theft, or fraud. Such internal controls must include the following:

a. All counts must be performed by at least two employees.

b. At no time during the count can there be fewer than two count team employees in the count room until the drop proceeds have been accepted into cage accountability.

c. Functions performed by count team employees must be rotated on a routine basis.

d. Count team employees must be independent of the Main Cage Function. A cage employee may be used if they are not the sole recorder of the count and do not participate in the transfer of drop proceeds to the cage. An accounting employee may be used if there is an independent audit of all count documentation.

12.5.3. A list of employees authorized to participate in the count and those employees who are authorized to be in the count room during the count (count personnel list) shall be maintained and available to the Commission upon request.

12.6. **Wagering Equipment**

12.6.1. **ADA Compliance**

Procedures shall be documented in the internal controls to ensure accessibility requirements defined by the Commission are met for the installation of Wagering Equipment in the Authorized Location. Accordingly, the Authorized Location is subject to the requirements of title III of the Americans with Disabilities Act of 1990, 42 U.S.C. §§ 12181-12189 ("ADA"), and its implementing regulations, which are found at 28 C.F.R. part 36.

12.6.2. **Shipping and Receiving**

Software and hardware components must be shipped in a secure manner to deter unauthorized access.

a. A communication procedure must be established between the Supplier, the Authorized Location, and the Commission to properly control the shipping and receiving of all software and hardware components. Such procedures must include:
   i. Notification of pending shipments must be provided to the Commission by the Authorized Location;
   ii. Certification by an independent test laboratory;
   iii. Notification from the Supplier to the Commission, or the Authorized Location as approved by the Commission, of the shipping date and expected date of delivery. The shipping notification must include:
      1) Name and address of the Supplier;
      2) Description of shipment;
      3) For hardware: serial number;
      4) For software: software version and description of software;
      5) Method of shipment; and
      6) Expected date of delivery.

b. Procedures must be implemented for the software and hardware components for maintenance and replacement.

c. The Commission, or its designee, must be present when an Authorized Location receives all hardware components e.g., Kiosks to verify the contents against the shipping notification.

12.6.3. **Location and Security**

The Authorized Location shall provide a secure location within the Commonwealth, or a location approved by the Commission in accordance with all applicable local and federal laws for the placement, operation, and usage of Wagering Equipment, including Ticket Writer Stations, Kiosks, displays, and communications equipment.

a. The Operator shall submit to the Commission, a current detailed floorplan, drawn to scale, depicting the secure location for the placement, operation, and use of all Wagering Equipment in the Authorized Location. The floorplan shall also include the surveillance camera coverage and the money routes.

b. Any proposed changes and re-locations of Wagering Equipment shall be submitted on subsequent floorplans in which Wagering Equipment is identified by location number(s).

c. Unless otherwise authorized by the Commission, Wagering Equipment shall have location numbers affixed to the outside and of sufficient height and size to be clearly visible and readable by the CCTV System;

d. At a minimum the following tasks should be performed on a scheduled basis:
   i. Clean out temporary files on hard disk drives;
   ii. Check hard disk space usage to ensure sufficient space is available for continued operations;
   iii. Check that all scheduled tasks are running correctly;
   iv. Check event logs for system, application, security, browser, DNS, and other errors; and
   v. Check UPS systems.

e. Internal controls shall be in place to prevent any person from tampering with or interfering with the operation of any wagering or Wagering Equipment

f. The Operator, subject to the approval of the Commission, must develop and implement physical security controls over the Wagering Equipment. These controls must address the following: forced entry, evidence of any entry, and protection of circuit boards containing programs.

g. The Operator must develop and implement procedures within the internal controls to ensure that data traffic communications between the Wagering Equipment and Sports Betting System is securely protected and functioning and that the integrity of the transactions is implemented

12.6.4. **Installation**

Testing must be completed during the installation process to verify that the Wagering Equipment components have been properly installed and that that the correct version of software is in place. This must include testing of the following, as applicable:

a. Communication with the Sports Betting System;
b. For Kiosks, currency and vouchers to bill validator;
c. Wager ticket and voucher printing;
d. Meter incrimination;
e. All buttons, to ensure that all are operational and programmed appropriately;
f. System components, to ensure that they are safely installed at location; and
g. Locks, to ensure that they are secure and functioning.

12.6.5. **Maintenance**

There must be effective maintenance planned to service Wagering Equipment, including computer program updates, hardware servicing.

a. The internal controls in respect of maintenance must include, but not be limited to, the following:
    i. Procedures in respect of maintenance of Wagering Equipment at all Authorized Locations.
    ii. Procedures for the detection of Wagering Equipment malfunctions.
b. Wagering Equipment maintenance must be independent of the Sports Betting Function.
c. Maintenance employees must report irregularities to management independent of the Sports Betting Function.
d. If the Wagering Equipment utilizes a barcode or microchip reader, the reader must be tested at least annually by employees independent of the Sports Betting Function to determine that it is correctly reading the barcode or microchip.

12.6.6. **Malfunctions**

The internal controls in respect of malfunctions of the Wagering Equipment and Sports Betting System must include, but not be limited to, the following:

a. Procedures to investigate, document and resolve malfunctions. Such procedures shall be delineated in the internal controls and must address the following
    i. Disabling and powering down the Wagering Equipment until repaired
    ii. Determination of the event causing the malfunction;
    iii. Review of relevant records, reports, logs, surveillance records;
    iv. Repair or replacement of the Wagering Equipment; and
    v. Verification of the integrity of the Wagering Equipment before restoring it to operation.
b. Procedures in the event of a communication malfunction occurring between the Sports Betting System and the Wagering Equipment which cannot be repaired immediately, and the reporting thereof to the Commission in writing within five (5) days; and
c. Procedures in the event that a malfunction is detected by the Commission and the Wagering Equipment disabled until such time that the malfunction has been repaired.

12.6.7. **Removal, Retirement and/or Destruction**

When not in use Wagering Equipment shall be stored in a location which is secure and only accessible by authorized personnel staff.

a. The Commission shall be notified in advance that the machines will be moved to the secure location. The notification must include the location of where the machines will be stored and the serial number or other unique number assigned to each machine that is being moved.
b. Procedures must be delineated in the internal controls and implemented to retire or remove any or all associated Wagering Equipment or components from operation. Procedures must include the following:
    i. For Wagering Equipment or components that accept financial instruments:
        1) Coordinate with the drop team to perform a final drop;
        2) Collect final accounting information such as meter readings, drop and payouts;
        3) Remove and/or secure any or all associated equipment such as locks, card reader, or printer from the retired or removed component; and

4) Document removal, retirement, and/or destruction.

ii. For removal of software components:

1) Uninstall and/or return the software to the Operator; and

2) Document the removal.

iii. For all components:

1) Verify that unique identifiers, and descriptions of removed/retired components are recorded as part of the retirement documentation;

2) Coordinate with the Accounting Function to properly retire the component in the system records.

c. Where the Commission authorizes destruction of any Wagering Equipment or components, procedures must be developed to destroy such components. Such procedures must include the following:

i. Methods of destruction;

ii. Witness or surveillance of destruction;

iii. Documentation of all components destroyed; and

iv. Signatures of personnel(s) destroying components attesting to destruction.

d. The internal controls in respect of the commissioning, alteration and de-commissioning of Wagering Equipment must include the following:

i. Procedures of the tests that must be performed as contemplated in the Rules whenever Wagering Equipment is moved or relocated from their initial locations to new locations at the site.

ii. Procedures to ensure that the Sports Betting System is immediately updated to reflect any commissioning, alteration or de-commissioning of Wagering Equipment at the time of such occurrence.

iii. Procedures for the recording of the results of these tests, which include that such record be signed by a representative from the Operator's designated function, as approved in their internal controls.

iv. Control measures for the maintenance of significant events and meter test documentation, including system reports in respect of the tests contemplated in the Rules for a period of at least five (5) years, for Commission inspection.

v. Completion of full data collection by the Sports Betting System prior to de-commissioning Wagering Equipment.

vi. That Wagering Equipment may not be exposed for use before the tests have been successfully completed and the information on the Sports Betting System has been verified as being correct.

12.7. **Communications Technology**

12.7.1. Before installing or permitting the installation of any communications technology, the Operator shall notify the Commission in writing of the location and number or other identifier of each communications technology and shall obtain the approval of the Commission for each communications technology. The Commission may condition the approval in any manner the Commission considers appropriate.

12.7.2. Before an Operator accepts any wagers, the Operator must obtain the written approval of the Commission to accept such wagers, and thereafter use only the communications technology approved for that purpose. Upon request, the Operator must provide the Commission with documentation of their communications technology.

12.7.3. As a condition to the granting of the privilege of having the communications technology, the Operator shall be deemed to have consented to the authority of the Commission to require the immediate removal of any communications technology at any time without prior notice of hearing. After any such removal, the Operator may request a hearing before the Commission as to whether or not circumstances may warrant the permanent revocation of the privilege of having communications technology upon the Authorized Location.

12.7.4. Upon the request of either the Commission, an Operator shall provide a written consent for the Commission to examine and copy the records of any telephone, telegraph, or other communications company or utility that pertain to the operation of the Operator.

12.8. **Key Controls**

12.8.1. Sensitive keys are those keys that either management or the Commission designates sensitive to the Operator's operation and therefore require strict control over storage, duplication, custody, issuance and return. Sensitive key procedures may be automated and/or manual.

a. Sensitive keys which require issuance under security or management escort must be identified as such in the key access list, including:

i. Unique identifier for each individual key;

ii. Key storage location;

iii. Number of keys made, duplicated, and destroyed; and

iv. Authorization and access.

b. Physical inventories of sensitive keys must be conducted quarterly to ensure that the physical count and the access list count match.

c. The internal controls must identify the employee responsible for conducting the physical inventories of sensitive keys.

d. The internal controls must identify which management employee has the authority to make changes, deletions and/or additions to the key access list.

12.8.2. The Operator shall establish and include in its approved internal controls, procedures to safeguard the use, access, and security of keys. The internal controls must include the:

a. Location of all sensitive key boxes and whether any of the boxes are portable or controlled by dual locks;

b. Job titles which have authorized access to the sensitive key box key(s) and how the keys to the sensitive key boxes are issued and controlled;

c. Sensitive key name, location, custodian and job titles authorized to sign out each sensitive key; and

d. Location and custodian of duplicate sensitive keys.

12.8.3. If key rings are used, each key ring and each key on the ring must be individually identified on the key access list maintained at each sensitive key box.

12.8.4. Each sensitive key box must be under surveillance coverage.

12.8.5. Each sensitive key box custodian must be issued a key access list noting authorized job titles that may access each key.

12.8.6. Whenever two sensitive keys are required to access a controlled area, the keys must be independently issued to different employees.

12.8.7. Access to and return of keys or equivalents must be documented with the date, time, and signature or other unique identifier of the employee accessing or returning the key(s).

12.8.8. The following requirements may apply for keys used in the drop and count process:

a. At least two (or more if required by the Commission) drop team employees are required to be present to access and return keys.

b. At least two (or more if required by the Commission) count team employees are required to be present at the time count room and other count keys are issued for the count.

c. Custody of all keys involved in the drop and count must be maintained by personnel independent of the count and the drop employees as well as those functions being dropped and counted.

d. Any use of keys at times other than the scheduled drop and count must be properly authorized and documented.

12.8.9. Emergency manual keys, such as an override key, for computerized, electronic, and alternative key systems must be maintained in accordance with the following (or as otherwise required by the Commission):

a. Access to the emergency manual key(s) used to access the box containing the Kiosk drop and count keys requires the physical involvement of at least two employees from separate functions, including management. The date, time, and reason for access, must be documented with the signatures of all participating persons signing out/in the emergency manual key(s);

b. The custody of the emergency manual keys requires the presence of two employees from separate functions from the time of their issuance until the time of their return; and

c. Routine physical maintenance that requires access to the emergency manual key(s) and does not involve accessing the Kiosk drop and count keys, only requires the presence of two employees from separate functions. The date, time, and reason for access must be documented with the signatures of all participating employees signing out/in the emergency manual key(s).

12.9. Security and Surveillance

12.9.1. Authorized Location Security

An Authorized Location shall be designed to promote optimum security for Sports Betting. The Operator shall submit a security and surveillance plan for Commission approval prior to accepting wagers in any approved Authorized Location. Any changes to the security and surveillance plan must be approved by the Commission.

12.9.2. Identification Badges

Identification badges issued by the Commission shall be worn by the Operator or Authorized Location employee, officer or director in a clearly visible location above the waist, while the employee, officer or director is present within the Authorized Location.

12.9.3. **Policy on Personnel Protection**

The internal controls shall delineate procedures to ensure that all personnel are receiving an adequate level of protection with regard to both their safety and security, including

a. Personnel working remotely outside Authorized Location
b. Personnel working inside the Authorized Location areas with public access

12.9.4. **Prevent Wagering by Prohibited Players or Intoxicated and Impaired Persons**

The Operator shall establish procedures to reasonably ensure a Prohibited Player or a player who is in a state of intoxication or is otherwise impaired is prohibited from participating in Sports Betting and such procedures are delineated within the internal controls. Once aware that a Prohibited Player or an intoxicated or impaired person is in the Authorized Location, the employee shall immediately notify security to remove them from the Authorized Location**.**

12.9.5. **Closed Circuit Television (CCTV) Systems**

The Operator shall establish a CCTV System to monitor sports betting operations conducted within an Authorized Location. For sports betting operations at a Casino or Racetrack, the CCTV System may be the same CCTV System used for other forms of gambling. At the Operator's discretion, the CCTV System requirements may be different for the sports betting operations at a Point of Sale or Satellite. The size and scope of CCTV Systems may vary depending on the number of Kiosks and Ticket Writer Stations for each Authorized Location.

a. The operation of Surveillance Personnel for the CCTV system shall be delineated within the internal controls.
b. The Operator and the Commission shall have free access to the CCTV System of the Authorized Location and its transmissions;
    i. For sports betting operations at a Point of Sale or Satellite, the CCTV System must be maintained and operated from a secured location, such as a locked cabinet.
    ii. For sports betting operations at a Casino or Racetrack, the CCTV System must be maintained and operated from a staffed surveillance operation room(s).
        1) The surveillance operation room(s) must be secured to prevent unauthorized entry.
        2) Access to the surveillance operation room(s) must be limited to surveillance personnel and other authorized persons.
        3) Surveillance operation room(s) access logs must be maintained.
        4) Surveillance operation room equipment must have total override capability over all other satellite surveillance equipment.
c. The cameras must be installed in a manner that will prevent it from being readily obstructed, tampered with, or disabled;
d. The CCTV System must:
    i. Monitor and record a general overview of
        1) Activities occurring in the main cage with sufficient clarity to identify individuals within the cage and players and personnel at the counter areas and to confirm the amount of each cash transaction;
        2) Activities occurring at Kiosks and Ticket Writer Stations with sufficient clarity to identify the activity and the individuals performing it, including maintenance, drops or fills, and redemption of wager tickets, vouchers or credits
        3) All areas where cash or cash equivalents may be stored or counted with sufficient clarity to provide coverage of count equipment and to view any attempted manipulation of the recorded data.
    ii. Record an accurate date and time stamp on recorded events. The displayed date and time must not significantly obstruct the recorded view;
    iii. Include sufficient numbers of recording devices to record the views of all cameras and have the capacity to display all camera views on a monitor
    iv. For sports betting operations at a Casino or Racetrack, include sufficient numbers of monitors to simultaneously display sports betting and count activities.
e. Recordings of sports betting operations shall be retained for a minimum of 90 days from the date of recording, unless the Operator gives instructions to keep them for a longer period of time. In addition, recordings related to suspected crimes, suspicious activity, or detentions by security personnel discovered within the initial retention period must be copied and retained for a time period, not less than one year.
f. Logs must be maintained and demonstrate the following:
    i. Compliance with the storage, identification, and retention standards;
    ii. Each malfunction and repair of the CCTV System; and

iii. Activities performed by surveillance personnel as required by these MICS.

g. In the event of power loss to the CCTV System
   i. For sports betting operations at a Point of Sale or Satellite, alternative security procedures, such as additional supervisors or security personnel, must be implemented immediately.
   ii. For sports betting operations at a Casino and Racetrack, an auxiliary or backup power source must be available and capable of providing immediate restoration of power to the CCTV System to ensure that surveillance personnel can observe all areas covered by dedicated cameras.

h. During the period of time that the Authorized Location is open to the public, there shall be adequate lighting and continued surveillance of sports betting operations

i. The Operator may, at its discretion, require that the CCTV System of the Authorized Location be connected to the Operator's offices through a Virtual Private Network (VPN), so that representatives of the Operator can observe the surveillance that is carried out in the Authorized Location in real time.

j. A periodic inspection of the CCTV Systems must be conducted. When a malfunction of the CCTV System is discovered, the malfunction and necessary repairs must be documented, and repairs must be initiated within seventy-two (72) hours.
   i. If a dedicated camera malfunctions, alternative security procedures, such as additional supervisors or security personnel, must be implemented immediately.
   ii. The Commission must be notified of any CCTV System and/or camera(s) that have malfunctioned for more than twenty-four (24) hours and the alternative security measures being implemented.

12.10. **Power Outages**

It is the responsibility of the Operator's security personnel to ensure that all players, employees and company assets are safeguarded against incidents that may occur during a power outage.

a. At a minimum, security representatives shall be dispatched to the following areas:
   i. All cages, satellite cages and betting counters;
   ii. Tops and bottoms of escalators, stairwells and elevators;
   iii. Count room(s) if count(s) are in progress; and
   iv. All other sensitive areas.

b. No money escorts of any kind shall be conducted during a complete power outage and any unsecured financial instruments in the Authorized Location shall be immediately returned to a secured area.

c. The Commission shall be informed immediately of any power outage.

Section 13.0 Player Account Management

13.1. **Player Account Procedures**

13.1.1. There shall be a formal process delineated within the internal controls for identification, authentication and authorization of a player. Procedures to address in the internal controls include, as applicable, but are not limited to:

a. The creation and use of Player Accounts, provided, that said accounts may not be owned by minors or on behalf of a beneficiary, custodian, trust, society, association or other organization or entity, nor may they be transferable, assigned or assigned to another person;

b. The creation and maintenance of documents related to the establishment of Player Accounts.

c. The exclusion of people not eligible for Sports Betting due to age, or because of their inclusion in the list of excluded people maintained by the Commission that has been distributed to the Operator at least five (5) days in advance to the effectiveness of the prohibition;

d. The acceptance of wagers including, but not limited to:
   i. Method of wagering communications;
   ii. Player account transactions documentation (creation and maintenance thereof);

13.1.2. Within an Authorized Location, Player Accounts must be established, maintained, and accounted for at one designated area. There shall be a procedure in place to ensure Player provides all information requested on the registration form. Further, all subsequent deposits/withdrawals and account adjustment transactions must be accounted for through the same designated area.

13.2. **Registration and Verification of Players**

13.2.1. The Operator shall have an identity verification process as a part of its registration process which may include requiring the use of a reputable independent Identity Verification Service Provider that is common in the business of verifying an individual's PII.

13.2.2. The Operator shall provide the Commission information about its procedures or methodology for verifying the identity of a player, including the legal name, physical address and age, and that the player is not on any Prohibited Player lists held by the Operator or the Commission.

13.2.3. The Operator shall notify Commission of any changes to its verification procedures or in the event there is a change of an Identity Verification Service Provider, as applicable. The verification procedures performed by the Operator are to be recorded and maintained which is to include the following information

a. If an Identity Verification Service Provider performs the verification process, the third-party service provider's verification results and verification date;

b. If not using an Identity Verification Service Provider or if the player's registration information does not result in a positive verification, the type of identification credential provided by the player, the last four digits of the relevant credential number, expiration date of credential, date credential was examined; and

c. Multi-sourced authentication, which may include third-party and governmental databases, used to verify the accuracy of the information provided for the player's date of birth and the physical address where the player resides.

13.2.4. The verification procedures are to involve robust identification methods to mitigate the risks of non-face-to-face transactions inherent in sports betting. However, the Identity Verification Service Provider may require a player to provide additional information, provide copies of documents, in order to complete the registration process.

13.2.5. The Operator shall establish procedures for handling the unsuccessful verification of the information provided by an individual who is registering as a player. Such procedures are delineated within the internal controls. The Operator is to record and maintain the following information:

a. Unique player ID and player name;

b. The date the account was suspended from further sports betting by the player;

c. The date the account was closed;

d. The amount of winnings retained which were attributable to the player; and

e. Balance of amount refunded to the player.

13.2.6. The Operator shall notify the player of the establishment of the Player Account by email and/or mobile phone number obtained during the registration process.

13.3. **Protection of Player Accounts**

13.3.1. The Operator shall implement internal controls and procedures to prohibit an individual, group of individuals, or entity that places wagers with the Operator from establishing more than one active Player Account with the Operator.

13.3.2. Procedures shall be in place to provide establish a secure personal identification for the player authorized to use the Player Account that is reasonably designed to prevent the unauthorized access to, or use of, the Player Account by any individual other than the player for whom the Player Account is established.

a. The Player Account shall be automatically locked-out after three failed access attempts in a thirty-minute period. A multi-factor authentication process shall be employed for the account to be unlocked or to recover or reset a password or username.

b. Internal controls shall be in place to ensure the strength of Player's passwords;

c. Player Accounts shall be immediately suspended, and Player's identification shall be immediately re-verified upon reasonable suspicion that the Player's identification has been compromised;

d. The internal controls shall delineate how the Operator may require a player to change or update account information at any time, including the Player's username and password.

e. Multi-factor authentication shall be required before allowing a player to change their password, access/update PII, transfer funds, or to remove a player from the Operator's Self-Exclusion list. If e-mail is a component of this process, the procedures for the secure use of e-mail as a medium for communicating secure information must be documented in the internal controls. The Operator shall develop alternative procedures for use in the event that a player no longer has access to the e-mail address on record.

f. A mechanism shall be in place to suspend a Player Account in the event that there is suspicion that the Player Account has been compromised or used to commit fraud or other illegal activity.

13.4. **Personally Identifiable Information (PII) Security**

13.4.1. Personally identifiable information (PII) shall be considered as critical assets for the purposes of risk assessment. This includes, but is not limited to:

a. The amount of money credited to, debited from, or present in any particular player account;

b. The amount of money wagered by a particular player on any Sports Event or Special Event;

c. The account number and authentication credentials that identify the player; and

d. The name, address, and other information in the possession of the operator that would identify the player to anyone other than the Commission or the operator.

13.4.2. There shall be procedures delineated in the internal controls for the security and sharing of PII as required by the Commission, including, but not limited to:

a. The designation and identification of one or more employees having primary responsibility for the design, implementation and ongoing evaluation of such procedures and practices;
b. The procedures to be used to determine
   i. The nature and scope of all PII collected
   ii. The purpose and legal basis for PII collection including, where required by the Commission, the "legitimate interest" pursued by the operator (or third-party service provider(s)) if this is the legal basis chosen (i.e., identification of the specific interest in question);
   iii. The locations in which the PII is stored, and the storage devices on which the PII may be recorded for purposes of storage or transfer;
   iv. The period in which the PII is stored, or, if no period can be possibly set, the criteria used to set this;
   v. For PII collected directly from the player, whether there is a legal or contractual obligation to provide the PII and the consequences of not providing that PII;
c. The measures to be utilized to protect information from unauthorized access;
d. The procedures to be used in the event the Operator determines that a breach of data security has occurred, including required notification to the Commission.

13.4.3. Where required by the Commission, players shall be provided with a method to request:
a. Confirmation that their PII is being processed;
b. Access to a copy of their PII as well as any other information about the PII processing;
c. Updates to their PII; and
d. Their PII erased and/or to impose restrictions on processing of PII.

13.4.4. There shall be procedures in place to record and process such requests from players, including maintaining records of such requests and providing reasons to the player when such requests are denied or rejected. The player shall be given a reason when the operator does not intend to comply with the request and also provided with the necessary information on the possibility to file a complaint with the Commission.

13.4.5. Where required by the Commission and upon player's request, the operator shall forward to the players the PII which they have received from the same player, in a structured, commonly used and machine-readable format and transmit those data to another operator, where it is technically feasible to do so. This only applies to:
a. PII which the player has provided to the operator or PII which is processed by automated means (i.e., this would exclude any paper records); and
b. Cases where the basis for processing is PII consent, or that the data is being processed to fulfil a contract or steps preparatory to a contract.

13.4.6. Where required by the Commission, the player has the right to object to PII processing and/or withdraw consent, if the processing is based on consent:
a. Based on legitimate interests or the performance of a task in the public interest or in the exercise of official authority;
b. Used in direct marketing, including profiling to the extent that it is related to such marketing activities; and
c. For scientific or historical research purposes or for the purpose of statistics.

13.4.7. There shall be procedures in place for the operator to comply with requests from players to have PII erased and/or to prevent or restrict processing of PII, including, in the following circumstances:
a. Where the PII is no longer necessary in relation to the purpose for which it was originally collected/processed;
b. When the player withdraws consent;
c. When the player objects to the PII processing and there is no overriding legitimate interest for continuing the processing;
d. The PII was unlawfully processed; or
e. The PII has to be erased in order to comply with a legal obligation.

13.4.8. Where applicable, the player shall be provided with information on the Operator's use of automated decision-making, including profiling and at least in those cases, without hindering compliance with other legal obligations:
a. Sufficient insight into the logic of the automated decision-making;
b. The significance and the envisaged consequences of such processing for the player; and
c. Safeguards in place around solely automated decision-making, including information for a player on how to contest the decision and to require direct human review or intervention.

13.4.9. Where prohibited by the Commission, the operator may not utilize solely automated decision-making which:
a. Produces legal effects the player such as those which result in the player being subjected to surveillance by a competent authority; or
b. Significantly affects the player in a similar manner (e.g., it has the potential to influence the circumstances, behavior or choices of the player).

13.5. **Payment Service Providers**

13.5.1. The Operator or Payment Service Provider (PSP) used to conduct transactions with financial institutions shall undergo a specific annual audit against common cybersecurity and information security principles in relation to the provision and use of payment services, as covered within these MICS. It is acceptable to leverage the results of prior audits conducted by appropriately accredited vendors and qualified individuals, within the current audit period (e.g., within the past year), against standards such as the Payment Card Industry Data Security Standards (PCI-DSS) or equivalent. Such leveraging will be noted in the audit report.

13.5.2. The Operator or PSP shall establish procedures to protect payment types used in the system from fraudulent use. Such procedures are delineated within the internal controls

a. Collection of PII and other sensitive information directly related to deposit/withdrawal transactions shall be limited to only the information strictly needed for the transaction.
b. There shall be processes in place for verifying the protection of the PII or other sensitive information directly related to each deposit/withdrawal transaction.
c. Any communication channels between the Operator and the PSP conveying deposit/withdrawal details shall be encrypted and protected against interception.
d. All financial transactions shall be reconciled between the Operator and the PSP daily. There shall be established procedures for:
    i. In calculating amounts paid to or received from a player, considering all payment types used by the player or Operator; and
    ii. Assuring the match of ownership between the payment type holder and the Player Account holder so as to avoid fraud and money laundering.

13.6. **Player Funds Maintenance**

13.6.1. **Player Funds Protection**

Funds held within Player Accounts may not be used as security by the Operator for any financial transactions and shall be considered as critical assets for the purposes of risk assessment.

13.6.2. **Financial Transactions**

Prior to the player making a deposit or withdrawal from a Player Account, the employee or Sports Betting System must verify the Player Account, the player identity, and availability of funds.

a. The player shall be provided confirmation/denial of every deposit/withdrawal transaction initiated, including:
    i. The type of transaction (deposit/withdrawal);
    ii. The transaction value; and
    iii. For denied transactions, a reason as to why the transaction did not complete as initiated.
b. A record of each deposit/withdrawal/adjustment is created and maintained that details the following information:
    i. Unique player ID and player name;
    ii. The type of transaction (e.g., deposit, withdrawal, adjustment);
    iii. The date and time of the transaction;
    iv. Unique transaction ID;
    v. The amount of transaction;
    vi. The total account balance before/after transaction;
    vii. The total amount of fees paid for transaction (if applicable);
    viii. User identification of employee or unique Wagering Equipment ID which handled the transaction (if applicable);
    ix. Method of deposit or withdrawal;
    x. Deposit authorization number;
    xi. Relevant location information;
    xii. Player signature for withdrawals, unless a secured method of access is utilized; and
    xiii. For adjustments to the account, the reason for the adjustment;
c. The Operator shall describe the sequence of the required signatures attesting to the accuracy of the information contained on the player deposit or withdrawal form ensuring that the form is signed by the cashier.
d. All player deposits and withdrawal transactions at the cage shall be recorded on a cage accountability form on a per-shift basis.
e. The Operator shall establish and comply with procedures that:
    i. Maintain a detailed record by Player Account and date of all funds on deposit;
    ii. Maintain a current balance of all player deposits that are in the cage/count room inventory or accountability; and

iii. Reconcile this current balance with the deposits and withdrawals at least daily.

f. Where financial transactions are allowed through the Electronic Funds Transfers (EFT), the Operator shall have security measures and controls to prevent EFT fraud. A failed EFT attempt shall not be considered fraudulent if the player has successfully deposited funds via an ACH transfer on a previous occasion with no outstanding chargebacks. Otherwise, the Operator shall:

i. Temporarily block the Player Account for investigation of fraud after five (5) consecutive failed EFT attempts within a ten (10) minute period. If there is no evidence of fraud, the block may be vacated; and

ii. Suspend the Player Account after five (5) additional consecutive-failed ACH attempts within a ten (10) minute period.

g. If EFTs are made to or from an operator's bank account for Player Account funds, the bank account must be dedicated and may not be used for any other types of transactions.

h. The internal controls shall delineate how the Operator may require players to provide additional information, provide copies of documents, or appear in person at the Authorized Location before processing a deposit or withdrawal. Players may also be required to complete additional Claim forms and/or certify documentation detailing their deposits, withdrawals, and other Player Account transactions.

i. The internal controls shall delineate how the Operator may withhold incorrectly deposited amounts from any deposit or prize or seek recovery if a player withdraws funds that were incorrectly credited to their Player Account.

13.6.3. **Deposits**

Procedures shall be established for the use of a PSP to allow the Operator to fund a Player Account

iii. The internal controls shall describe a complete description of the entire process for each deposit method, including situations where additional information must be requested prior to completing the deposit transaction;

iv. The routing procedures for deposits by mail require that the mail deposits are received by a function independent of the Sports Betting Function.

13.6.4. **Withdrawals**

Procedures shall be established for the use of a PSP to allow the Operator to remove funds from a Player Account**.**

a. The internal controls shall describe a complete description of the entire process for each withdrawal method, including situations where additional information must be requested prior to completing the withdrawal transaction;

b. Prior to any withdrawal, if a player used a credit or debit card to fund a Player Account, any remaining balance in the Player Account up to the amount of the deposit shall be refunded to the player's credit or debit card account used to fund the Player Account provided that a credit or debit card issuer permits the return of a withdrawal from a Player Account funded by the credit or debit card of the issuer.

c. Sports Betting Systems shall employ a mechanism that can detect and prevent any player-initiated withdrawal activity that would result in a negative balance of a Player Account

d. Direct access to a Player Account to withdraw funds is restricted to the player who owns the Player Account and who is confirmed to be the owner by using positive player identification methods such as a PIN number or password. *The Customer Service function may be able to reset the PIN number or password for a Player Account in the system to permit a person with legal authority to gain access to the Player Account when the owner of the account is incapacitated or deceased. For this occurrence, sufficient records are maintained evidencing the reason for resetting the PIN number or password.*

e. Indirect access (i.e., player is not providing a PIN number or password) to a Player Account to withdraw funds involves assisted access by a member of the Customer Service function whether online or by other means. The employee who is assisting with an indirect access is to use challenge questions to identify the person making remote access or employ a sufficient alternative process to ensure that the person is accurately identified as the owner of the Player Account. If challenge questions are used, the responses to challenge questions should be obtained during the registration process for a Player Account.

13.6.5. **Adjustments**

The internal controls shall delineate how the Operator may make the appropriate adjustments to a Player Account if funds are mistakenly credited to or deducted from the Account.

a. The Operator shall have security or authorization procedures in place to ensure that only authorized adjustments can be made to Player Accounts, and these changes are auditable.

i. All adjustments under $500 shall be periodically reviewed by supervisory personnel.

ii. All other adjustments shall be authorized by supervisory personnel prior to being entered.
iii. The internal controls shall identify the job titles of supervisory personnel authorized to perform this function and specify which evidence of supervisory authorization is to be recorded and maintained.

b. On a daily basis, supervisory personnel may authorize multiple transactions occurring within an operational day. Evidence of supervisory authorization for multiple transactions is to be recorded and maintained. The internal controls are to delineate the authorization process for multiple transactions rather than authorizing each individual transaction.

13.7. **Account Closure**

The Operator shall have internal controls, which permit an individual, group of individuals, or entity that places wagers with the Operator to terminate the account at any time and for any reason and without penalty.

a. The process for account closure must be simple. A player must be able to request the closure of their account through the Mobile App or Site, in addition to via email, telephone, and direct request at the Authorized Location.
b. A player must not be encouraged or induced to keep their account open following their request to close their account. However, an Operator may explain the effects of an account closure and ask the player if they wish to proceed.
c. The Operator shall offer a readily accessible method for a player to close his or her account at any time. The account closure process must commence immediately upon receipt of the account closure request
d. The account may remain in pending closure status if there are outstanding confirmed wagers, such as a wager on a future event. The account closure process must result in the account being closed after all wagers have been settled.
e. Any balance remaining in a Player Account closed by a player shall be refunded within five (5) business days pursuant to the internal controls, provided that the Operator acknowledges that the funds have cleared.

13.8. **Dormant and Closed Accounts**

Access to dormant and closed account information is restricted to those positions which require access and are so authorized by management. Such access is to be delineated within the internal controls.

Section 14.0 Reports and Information Storage

14.1. **Reporting Requirements**

The Sports Betting System shall generate the information needed to compile the following reports on demand, on a daily basis and a monthly basis as deemed necessary by the Commission. Such reports shall distinguish by type and status where applicable and be produced in a format approved by the Commission:

a. Wager Summary Reports that contain a summary of wagers on events, including those completed and those not completed, by event and in total for the period.
b. Win Summary Reports that contain a summary of winning wagers on events that were completed and confirmed by the end of the period, including completed payouts, and winning wager tickets not yet redeemed, by event and in total for the period.
c. Potential Payout Reports that contain a summary of potential payouts for wagers on events that were not completed and confirmed by the end of the period, by event and in total.
d. Account Financial Transaction Reports which contain the unique transaction identifier, the date and time of transaction and the amount of each deposit, withdrawal, or adjustment during the period, by Player Account and in total
e. Account Wagering Reports which contain the unique wager identifier, the date and time of wager, the amount of each wager, and (if a winner) the amount won during the period, by Player Account and in total
f. Ticket Wagering Reports which contain the unique wager identifier, the date and time of wager and the amount of each wager placed during the period, by issuing Wagering Equipment and in total
g. Winning Wager Ticket Redemption Reports which contain the unique wager identifier, the date and time of redemption and the amount of each winning wager ticket redeemed during the period, by redeeming Wagering Equipment and in total
h. Unredeemed Winning Wager Ticket Reports which contain the unique wager identifier, the date and time of being declared a winner, the expiration date, and the amount of each winning wager ticket that has not been paid
i. Voucher Issuance Reports which contain the unique voucher identifier, the date and time of issuance and the amount of each voucher issued during the period, by issuing Wagering Equipment and in total

j. Voucher Redemption Reports which contain the unique voucher identifier, the date and time of redemption and the amount of each voucher redeemed during the period, by redeeming Wagering Equipment and in total
k. Unredeemed Voucher Reports which contain the unique voucher identifier, the date and time of issuance, the expiration date, and the amount of each voucher that has not been paid
l. Player Account Balance Reports that contain, the opening and closing balances, and a summary of financial and wagering transactions during the period affecting those balances, including adjustments, by Player Account and in total.
m. Event Results Reports that contain lists, for each event the date and starting time of the event, the event (e.g., athlete or participant names and team identifications), and the event results/winners.
n. Sports Betting Operator Liability Reports that contain each amount listed under the Regulations for **"Operator Reserves"** and its total amount
o. Adjusted Gross Revenue Reports that contain the amounts for wagers, prizes, voids, cancellations, takeout or fees, and other expenses.
p. Sports Betting Statistical Reports which indicate the total amount of wagers accepted, total amount paid out on winning wagers, the net amount won by the book (i.e., taxable revenue), and the win-to-write percentage for each sport (e.g., baseball, basketball, football, hockey, golf, boxing, etc.) in order to ensure the integrity of operations related to operating a sports betting.
q. Voluntary Exclusion Reports that contain the total number of persons that requested to exclude themselves from sports betting including their names
r. Involuntary Exclusion Reports that contain a list of names of persons whom the Operator had excluded from sports betting including the reasons why the person was excluded

14.2. **Electronic Storage of Information**

Reports and other documents/records may be directly written to an electronic document retention system in a portable document format (PDF) or scanned to an electronic document retention system into either a portable document format or standard image format provided that the following items are met:

a. If scanned, documentation must be verified by at least one additional person when being added to the electronic document storage system to ensure that the scanned version is identical to the original document. The second person must provide an electronic signature or other method of sign-off verification with the date and time to demonstrate that the review was performed prior to the document being added to the system.
b. On a quarterly basis, internal audit personnel shall review a minimum of 20 documents added to the electronic document retention system.
    i. The review shall assess whether:
        1) The documents are accurate reproductions of the original and the hash signatures match to the signatures recorded when the documents were added to the system;
        2) The documents are readable and version control is functioning properly (i.e., all changes after the original was added are reflected in subsequent versions);
        3) Indexing is correct (i.e., all information is accurate, and the document is easily identified);
        4) User access to add or modify documents is set to an appropriate level of access to administer the electronic document retention system, and no terminated employees have active user accounts on the system;
        5) Event recording and reporting is functioning as designed and the logs are being reviewed by the appropriate personnel regularly; and
        6) Redundancy exists and is adequately functional to limit the level of risk that an outage or loss of records may occur in the event of hardware failure or other unforeseen event.
    ii. Evidence of the review shall be maintained for five years. The evidence is to include at a minimum:
        1) The date and time of review;
        2) Name and title of person performing the review;
        3) The document records reviewed; and
        4) Any exceptions, follow-up and resolution of exceptions.
a. The internal controls must delineate the name and components of the electronic storage system, all procedures used for electronic document retention and the titles for all employees responsible for administering and maintaining the system.

Section 15.0 Bank Secrecy Act (BSA) Compliance

15.1. **Transactions in Excess of $10,000**

The Operator shall establish and comply with, internal controls for the reporting of transactions in excess of $10,000 that appear to be transacted to avoid filing requirements of the Bank Secrecy Act, Title 31 (31 CFR, part 103). Compliance with the MICS does not release the Operator from its obligation to comply with all applicable local and federal regulations.

15.2. **Cash Transaction Report (CTR)**

15.2.1. The Operator shall file a Cash Transaction Report (CTR) with the Financial Crimes Enforcement Network (FinCEN) of each or multiple of the following types of transactions:

a. A wager of $10,000 or more;
b. A Player Account deposit of $10,000 or more;
c. A payout of $10,000 or more on a winning wager; or
d. A Player Account withdrawal of $10,000 or more.

15.2.2. Each type of transaction shall be aggregated separately in order to determine that the reporting threshold is met. The Operator shall monitor all transactions to ensure players are not circumventing these requirements.

15.2.3. Before concluding any transaction where an CTR is required to be filed, the Operator shall obtain and record the following information

a. The player's legal name;
b. The player's date of birth;
c. The player's residential address (a post office box is not acceptable);
d. The player's Social Security number or equivalent for a foreign player such as a passport or taxpayer identification number;

15.2.4. The information in MICS 15.2.3 can be pulled automatically, as well as the recorded document number of the government-issued identification credentials examined for player registration, or other methodology for remote, multi-sourced authentication, which may include third-party and governmental databases, as approved by the Commission

15.2.5. If the player is unable to provide an acceptable form of identification, the transaction must be refused until the necessary information has been obtained. If a player refuses to provide proper identification, when required by regulation or policy, all financial or wagering transactions will be stopped and the player will be barred from any further sports betting activity until satisfactory identification is provided.

15.2.6. Subsequent to processing a transaction in excess of $10,000 the Operator shall record on the CTR and maintain records that include:

a. The player's legal name;
b. The player's address;
c. The player's social security number;
d. A description including any document number of the identification credential examined;
e. The amount of the transaction;
f. The Ticket Writer number or other identification of the location where the transaction occurred;
g. The time and date of the transaction;
h. The names and signatures of the Operator employees accepting or approving transaction; and
i. Where possible, a surveillance photo of the player. Surveillance will be notified prior to the completion of the qualifying transaction and take at least one photograph of the player from the surveillance camera. The photo must include the player's name printed on the back, and the signatures of both the surveillance operator and the employee witnessing the transaction. When a photograph is not obtainable for an after the fact CTR, the employee completing the CTR will attach to the Operator's copy a written explanation that there was no photograph taken because it is an after the fact CTR.

15.2.7. If CTRs are prepared by sports betting personnel pursuant to MICS 15.2.7, the completed CTRs are submitted to the Accounting Function by no later than 24 hours.

15.2.8. CTRs shall be filed with FinCEN no later than 15 days following the day on which the reportable transaction occurred.. The Operator shall file an amended report if the Operator obtains information to correct or complete a previously submitted report, and the amended report shall reference to the previously submitted report. The Operator shall retain a copy of each report filed for at least 5 years unless the Commission requires retention for a longer period of time. Due to the sensitive content in these reports, all communication should be sent using an encryption process of encoding messages.

15.3. **Multiple Transactions Log (MTL)**

15.3.1. Before completing a transaction with a player that, when aggregated with others, totals more than $10,000 during any operational day, the Operator shall complete a Multiple Transactions Log (MTL) with identification and record keeping requirements described in MICS 15.2 above. Multiple transactions, of the same type or category, shall be

treated as single transaction if the Sports Betting System records the same type of transactions for a player totaling more than $10,000 during any single operational day.

15.3.2. The Operator shall not knowingly allow, and shall take reasonable steps to prevent, the circumvention of reporting requirements through a player making structured transactions, including multiple transactions or a series of transactions that are designed to accomplish indirectly that which could not be accomplished directly. A transaction or transactions need not exceed the dollar thresholds at any single Operator in any single day in order to constitute prohibited structuring. No Operator shall encourage or instruct the player to structure or attempt to structure transactions. This does not prohibit an Operator from informing a player of the regulatory requirements imposed upon the License, including the definition of structured transactions. An Operator shall not knowingly assist a player in structuring or attempting to structure transactions.

15.3.3. Within 24 hours after the end of a designated 24-hour period, MTLs created pursuant to MICS 15.3.1 are submitted to the Accounting/Compliance function.

Section 16.0 Anti-Money Laundering (AML) Compliance

16.1. **AML Compliance Policy**

The Operator shall submit to the Commission for approval a description of their comprehensive and robust AML compliance policy that is risk-based and will adequately address the risks posed by sports betting for the potential of money laundering and terrorist financing. At a minimum, the AML compliance policy shall provide for:

a. Internal controls to assure ongoing compliance with the local AML regulations and standards observed by the Commission which should be documented in writing containing the approval of senior management;

b. Up to date training of employees, including training in the identification of unusual or suspicious transactions, a clear reporting line and escalation path and the creation and maintenance of any records required to the extent that the reporting of such transactions is required by applicable law or regulation, or by the Operator's own administrative and compliance policies which includes, but is not limited to, records of the training curriculum, attendance records, and established pass/fail criteria for test results;

c. Assigning an individual or individuals and their responsibilities in relation to AML matters including reporting unusual or suspicious transactions and a clear procedure for the review and implementation of any compliance officer recommendations or reports;

d. The Operator may establish a suspicious activity compliance committee who shall meet periodically for assessment of Suspicious Activity Reports (SARs) prepared for determination of filing;

e. Monitoring Player Accounts for opening and closing in short time frames and for deposits and withdrawals without associated wagering transactions;

f. Ensuring that aggregate transactions over a defined period may require further due diligence checks and may be reportable to the relevant organization(s) if they exceed the threshold prescribed by the Commission.

g. Internal testing for compliance with the requirements of the sports betting and AML law;

h. Integrating and sharing data as appropriate and feasible among:

   i. Different parts of the Authorized Location;

   ii. Any other operators;

   iii. Other entities providing sports betting services; and

   iv. Affiliates in other jurisdictions;

i. Consideration of all remuneration and employee incentive policies and structures to ensure that no person is rewarded as a result of failing to comply with the AML compliance policy;

j. Procedures to ensure that high risk or politically exposed persons (PEPs) are identified so that appropriate sign-off is obtained for transactions involving those persons;

k. Procedures to implement such measures as are necessary to assist any law enforcement or regulatory authorities in the Commonwealth with any investigations or enabling those authorities to freeze or seize assets where permitted by law; and

l. The use of any automated data processing systems to monitor the variety, frequency and volume of transactions to aid in assuring compliance;

m. Procedures for using all available information to determine:

   i. The full name, date of birth, and residential address, and verification of the same, of a player, when required by the Commission or any other law enforcement agency to provide such information;

   ii. The occurrence of unusual or suspicious transactions; and

   iii. Whether a Suspicious Activity Report (SAR) needs to be filed pursuant to the Regulations

n. Annual internal and/or external independent testing for compliance which includes the maintenance of work papers, frequency of testing, scope of testing, results of testing, conclusions and notice to management of testing results. Logs of all tests shall be maintained.

16.2. **AML Risk Assessment**

The operator shall conduct a risk assessment to identify any areas of its sports betting operations at risk for money laundering and the AML compliance policy shall specify the measures to address those risks. The risk assessment shall cover, but not be limited to, the risks involving:

a. Players generally, which may include whether a player:
   i. Has sources of wealth or income commensurate with his sports betting activity;
   ii. Has provided personal, financial or business information that can be readily verified;
   iii. Has fiduciary obligations that may create a risk of misappropriation of funds;
   iv. Is associated with individuals or entities known to be connected to the illicit generation of funds or the laundering of such funds;
   v. Has been made bankrupt;
   vi. Has a prior history of criminal or dishonest conduct; or
   vii. Is a politically exposed person (PEP);
b. Sports betting generally;
c. Products and services offered by or on behalf of the operator;
d. Employees in the proper performance of their functions and duties and as a voluntary or involuntary part of any AML scheme;
e. The use of foreign holding accounts where funds are held in a foreign jurisdiction for use in an Authorized Location in the Commonwealth;
f. The use of third-party marketing agents and junkets;
g. The ownership structures and integrity of intermediaries and associated businesses such as junket promoters, agents, manufacturers, financial service providers;
h. Criminal activities and proceeds of crime generated domestically as well as generated abroad but laundered domestically;
i. Financial services offered by the operator or by an intermediary; and
j. The use of Wagering Equipment that accepts cash.

16.3. **AML Compliance Officer**

The operator shall ensure that it has at all times a compliance officer to assure day-to-day compliance and to be responsible for all areas of AML by the Operator. The compliance officer shall:

a. Be adequately trained to carry out the role, including reporting unusual or suspicious transactions
b. Fully understands the relevant AML requirements;
c. Be available to other employees to consult on AML related issues as they arise;
d. Be fully knowledgeable as to the operator's products, services, player base and particular AML risk areas; and
e. Have appropriate authority and resources to implement the operator's AML policies.
f. Be responsible for ensuring that training is provided at a minimum to the following general categories of employees:
   i. Those engaged in the sports betting operation;
   ii. All employees with cash or credit handling responsibilities;
   iii. Surveillance employees;
   iv. Employees in the accounts function;
   v. Senior management; and
   vi. Employees responsible for marketing or hosting high value players.

16.4. **AML Program Violation**

Each Operator shall notify the Commission within 24 hours upon discovery and knowledge of any material violation or non-compliance with the AML compliance program, policies, and procedures (e.g., failure to file a Currency Transaction Report (CTR) or Suspicious Activity Report (SAR)); AML laws or regulations; any regulatory compliance program, policies, and procedures; or any law or regulation governing the Operator in any jurisdiction, including the Commonwealth.

Section 17.0 Accounting and Auditing Procedures

17.1. **Accounting Controls**

Internal controls must be established, and procedures implemented to safeguard assets and ensure the Regulations for "**Financial and Compliance Auditing**" are met including accounting controls which provide reasonable assurance that:

a. Transactions or financial events pertaining to the revenues and expenses of a Sports Betting Operation are:

i. Executed in accordance with the Operator's authorization protocols;
ii. Recorded to permit preparation of financial statements consistent with Generally Accepted Accounting Principles (GAAP) in the United States, and the requirements of the Commission; and
iii. Recorded to permit proper and timely reporting and calculation of proceeds and to maintain accountability for assets;

b. Access to the Operator's facility and components thereof permitted only in accordance with the Operator's authorization protocols;
c. The recorded accountability for assets is compared with actual assets at least annually and appropriate action is taken with regard to a discrepancy; and
d. Procedures are submitted that detail the reconciliation of assets and records contained in a Ticket Writer Station's drawer, Kiosk, and Sports Betting System.

17.2. **Internal Audit Program**

The Operator must establish policies and procedures in connection with the internal audit program of its wagering operations, which ensures that:

a. Internal audit activities are conducted in a manner that permits objective evaluation of areas examined.
b. Internal Audit Compliance Checklists are developed and submitted to the Commission for approval, outlining Walk-Through Procedures and Testing Procedures to be performed on a daily, weekly, monthly, or quarterly basis to determine if internal controls comply with the applicable Regulations and MICS for the Operator.
c. Audit reports are maintained for a minimum of five years and are made available to the Commission upon request. Such audit reports shall include the following information:
   i. Audit objectives;
   ii. Audit procedures and scope, which include:
      1) Whether the test was performed by inquiry, observation or examination;
      2) The scope of each observation, review and test including the sample sizes and dates tested; and
      3) The population from which the sample is selected for testing purposes, including all transactions occurring subsequent to the prior period's test dates through the current period's test date. For example, if the test date for the first quarter was February 5, the population for the second quarter's audit must include all transactions from February 6 through June 30;
   iii. Findings and conclusions. The page number references to internal controls which correspond to findings must be included along with the specific number of exceptions noted. If there are no findings, the report must indicate that no audit findings were noted. All findings relating to the required internal audits and any other internal audits relating to sports betting operations must be reported. Non-sports betting related findings should not be included;
   iv. Recommendations, if applicable. All recommendations must be discussed with management prior to the report being submitted to the Commission;
   v. Observations. Exceptions noted that are not internal controls violations but relate to sports betting operations must be included; and
   vi. Management's response. This must include the specific corrective actions to be taken, implementation dates and the employees responsible for implementation and subsequent follow-up. Responses are required for findings. Responses are only required for observations if required by Authorized Location policy.
d. The internal audit report is delivered to management, the audit committee, the Commission upon request, or any other entity designated by the Operator.
e. All material instances of noncompliance identified by internal audit work are investigated and resolved and the results are documented and reported immediately to the Commission.
f. Follow-up observations and examinations are performed to verify that corrective action has been taken regarding all instances of non-compliance. The verification is performed within six (6) months following the date of notification of non-compliance.
g. Documentation (e.g., log, checklist, notation on reports, and tapes attached to original documents) is maintained evidencing the performance of sports betting audit procedures, the exceptions noted and follow-up of all sports betting audit exceptions as it relates to compliance with these MICS, including all instances of noncompliance.

SPORTS BETTING MICS

Section 19.0 Definitions

The following words and terms, when used in these Minimum Internal Control Standards (MICS) shall be in accordance with the Law, the Regulations, and GLI-33, and shall have the following meanings unless the context clearly indicates otherwise.

Access Control	The process of granting or denying specific requests for obtaining and using sensitive information and related services specific to a system; and to enter specific physical facilities which houses critical network or system infrastructure.
Accountability	All financial instruments, receivables, and Player Account deposits constituting the total amount for which the bankroll custodian is responsible at a given time.
Adjusted Gross Revenue	The Total Revenue Received by the operator from players in Puerto Rico minus the total sums paid to winning players in Puerto Rico. This includes the cash equivalent of any merchandise or object of value awarded as a prize, the free play offered and payments of the tax on the consumption of specific goods to the Federal Government of the United States of America.
Administrative Access	Access that would allow a user (i.e., system administrator) to: • Add, change, or delete user accounts and associated user provisioning for database, operating system, and network layers (may also include user access administrator function for an application layer); • Modify operating system, network, database, and application layers' security and policy parameters; • Add, change, or delete system exception logging information; or • Add, change, or delete permissions to data files, folders, libraries, tables, or databases.
Alcoholic Beverages	All substances known as ethylic alcohol, hydrated ethyl oxide, or wine spirits, which are commonly produced through the fermentation of grains, starch, molasses, sugar, sugar cane juice, beet juice, or any other substance that may be obtained through distillation, including all solutions and mixes of such substances that have been reduced to a potable proof for human consumption and the liquors and drinks that contain alcohol, whether produced through fermentation or distillation, including, but not limited to, beers, wines, and cider (Source: Article 5 of Law No. 143 of June 30, 1969, as amended).
Algorithm	A finite set of unambiguous instructions performed in a prescribed sequence to achieve a goal, especially a mathematical rule or procedure used to compute a desired result. Algorithms are the basis for most computer programming.
Anti-Money Laundering (AML)	The legal controls that require financial institutions and other regulated entities to prevent, detect and report money-laundering activities
Application	All the forms, documents and information that are required to be submitted or completed in order to obtain a license or permit.
Asset Number	A unique number permanently assigned to a Kiosk and a cash storage box for purposes of tracking that machine and storage box while used by an Operator.
Associated Equipment	Any computer or component thereof ("hardware") located in the places allowed by the Law, connected for communication, validation and other functions purposes to the system.
Athlete or Participant	An individual, team, or other entity whom a player selects for the purposes of a wager in Sports Betting.
Audit Trail	A record showing who has accessed a system and what operations the user has performed during a given period.
Authentication	Verifying the identity of a user, process, software package, or device, often as a prerequisite to allowing access to resources in a system.
Authorized Location	A physical establishment, be it a Principal Operator or a Satellite, that has a license issued by the Commission to accept and pay out winnings for sports bets from authorized players registered to carry them out.
Authorized Player or **Player**	An individual, 18 years of age or older, whose identity was authenticated and recorded through a means implemented by the operator which shall meet the intentions of the Law. Once the player is authorized, they can participate in any Sports Betting offered by that operator
Back-Office Platform	A component external to the kiosk terminal which may govern some or all the regulated operations of the kiosk, such as metering and communications between the Sports Betting System and the kiosk terminal. The back-office platform may be integrated into the Sports

	Betting System. For the purposes of these MICS, the Back-Office Platform is considered a part of the kiosk.
Backup	A copy of files and programs made to facilitate recovery if necessary.
Backup System Log	An event log, a job log or an activity file created by the program or batch process that performs backups of application and data files. These event logs, job logs or activity files usually provide detail on the type of backup performed, success or failure of the operation, and a list of errors.
Barcode	An optical machine-readable representation of data. An example is a barcode found on printed wager tickets or vouchers.
Bill Validator	A wagering equipment peripheral that accepts paper currency, vouchers, and winning wager tickets in exchange for credits.
Biometrics	A biological identification input, such as fingerprints or retina patterns.
Bonus or **Promotion**	Incentive that is added to the Player Account when a Player meets participation requirements in accordance with the applicable rules for the particular promotion.
Cage	A secure work area within the Authorized Location for Ticket Writers and cashiers, which may include a storage area for the Authorized Location bankroll.
Cage Cashier	Any person whose duties include working in a physical structure known as a main cage, a satellite cage, and who has custody of the cage inventory comprising financial instruments, forms, documents, and records normally associated with the operation of a cage and other functions normally associated with a cashier.
Cage Supervisor	Any person whose job requires that person to supervise personnel and functions within the main cage, but not to perform a role that would result in performing an incompatible function.
Cancelled Wager	A wager that has been cancelled due to any issue with an event that prevents its completion.
Cash Storage Box	An electromechanical bill validator component that loads paper currency, vouchers, and winning wager tickets into a locked container for secure storage within the Kiosk.
Closed Circuit Television (CCTV) System	A closed-circuit television, as described in these MICS, or any other technology that is authorized by the Commission.
Commission	The Puerto Rico Gaming Commission.
Commonwealth	The Commonwealth of Puerto Rico.
Communications Technology	Any method used and the components used to facilitate the transmission of information, including, without limitation, the transmission and reception by systems based on data networks with conducting or wireless wires, or cable , radio, microwave, light, optics or the computer, including, without limitation, the Internet and intranets.
Competitor	A participant in a match or event in an Esports competition.
Complainant	Person who imputes the commission of a violation of the Law or the Regulations, and requests that a right be recognized, or a remedy be granted.
Complaint	A written claim, duly sworn and presented by a Person before the Commission requesting that a right be recognized and / or a remedy be granted for any act or omission in violation of the Law, this Regulation or Order of the Commission.
Complimentary Services	Services or products, gifts, money or other items of value granted by the Operator to any person, directly or indirectly, at no cost or at a reduced price, including, among others, those granted by a raffle, promotion or tournament. Services may include, but are not limited to, travel, lodging, food, beverages, or entertainment expenses.
Confidential Information	All nonpublic proprietary information of the Operator or the Event, which is marked confidential, restricted, proprietary or with a similar designation, obtained as a result of the employment of a person or by virtue of it.
Confirmed	A Wager was placed by a Player, the system accepted the Wager, the Wager amount was successfully debited from the Player Account, the Wager was recorded by the system, and the Player received a printed or virtual wager ticket.
Contingency Plan	A plan for processing critical applications and preventing loss of data in the event of a major hardware or software failure or destruction of facilities.
Contractor	Any person or entity who works pursuant to an independent contract with the operator and who has access to non-public portions of the operator's office, to information on the operator's computer network that is not publicly available, or to operator proprietary information that may affect how the Sports Betting is played.

Count	The act of counting and recording the drop and/or other funds. Also, the total funds counted for a particular Kiosk, Ticket Writer Station, cashier, shift, or other period.
Count Room	A secured room where the count is performed in which financial instruments are counted.
Count Team	Personnel that perform the count of the Kiosk and Ticket Writer Station drop.
Counter Check	A form provided by the Authorized Location for the player to use in lieu of a personal check.
Critical Component	Any sub-system for which failure or compromise can lead to loss of player entitlements, government revenue or unauthorized access to data used for generating reports for the Commission. Examples of critical components include: • Components which record, store, process, share, transmit or retrieve PII and other sensitive information (e.g., validation numbers, authentication credentials, etc.); • Components which store results or the current state of a player's wager; • Points of entry to and exit from the above components (other systems which communicate directly with core critical systems); and • Communication networks which transmit PII and other sensitive information.
Critical Control Program	A software program that controls behaviors relative to any applicable technical standard and/or regulatory requirement.
Cryptographic Random Number Generator (RNG)	An RNG which is resistant to attack or compromise by an intelligent attacker with modern computational resources who has knowledge of the source code of the RNG and/or its algorithm. Cryptographic RNGs cannot be feasibly 'broken' to predict future values.
Data Integrity	The property that data is both accurate and consistent and has not been altered in an unauthorized manner in storage, during processing, and while in transit.
Data Processing Agreement	A written contract, or other binding legal document which sets out • The subject matter and duration of the processing; • The nature and purpose of the processing; • The type of data to be processed; • How the data is stored; • The detail of the security surrounding the data; • The means used to transfer the data from one organization to another; • The means used to retrieve data about certain individuals; • The method for ensuring a retention schedule is adhered to; • The means used to delete or dispose of the data; and • The categories of data.
Days	Calendar days unless otherwise specified. Whenever any provision of these MICS requires that an act or event take place on a specific day or date, and said day or date falls on a Saturday, Sunday, or official holiday, it shall be understood that said provision refers to the next business day following said day or date. When the term granted is less than 7 days, Saturdays, Sundays or intermediate legal holidays will be excluded from the calculation. A half day holiday will be considered a full holiday.
Debit Instrument	A card, code, or other device with which a person may initiate an electronic funds transfer. The term includes, without limitation, a prepaid access instrument.
Dedicated Camera	A video camera required by these MICS to continuously record a specific activity. In lieu of continuous recording, time-lapse recording is acceptable if approved, in advance, by the Executive Director or their designee.
Default Accounts	User accounts with predefined access levels usually created by default at installation for operating systems, databases, and applications. These accounts tend to be used for training purposes.
Deposit	Money a player adds to their Player Account and may be used to place wagers.
Domain	A group of computers and devices on a network that are administered as a unit with common rules and procedures.
Dormant Account	A Player Account which has had no player-initiated activity for a period of one (1) year.
Drop Proceeds	The amount of financial instruments in a Kiosk or Ticket Writer Station, if applicable.
Employee	A person employed in a sports betting operation and determined by the Executive Director to have employment duties and responsibilities involving the security, maintenance, servicing, repair, or operation of Wagering Equipment, or is employed in a position that allows direct access to the internal workings of Wagering Equipment. Such employees shall include,

	without limitation, Sports Betting IT staff, security and surveillance employees, and employees responsible for handling assets and proceeds associated with the sports betting operation.
Encryption	The conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized people.
Encryption Key	A cryptographic key that has been encrypted in order to disguise the value of the underlying plaintext.
Esports	Organized video game competition events in which individual competitors, from different leagues or teams compete against each other in popular games in the video game industry. There are three (3) modalities: (a) Events or tournaments of electronic sports, face-to-face or through the internet. (b) Skill Based Gaming - Combine chance with player skill. (c) Peer-to-Peer Gaming - Models traditional affairs, where two players play against each other and they compete through an intermediary, who pays the winner and collects a commission.
Esports Competition	A Special Event involving the competitive playing of video games between individual competitors.
Event	Occurrence related to Sports Events and Special Events approved by the Commission.
Executive Director	The Executive Director of the Gaming Commission of the Government of Puerto Rico.
External Wagering System	System hardware and software separate from that which comprises the Sports Betting System, which may drive the features common to wager offerings, wager configurations, reporting, etc. The player initially communicates directly with the Sports Betting System which can be integrated with one or more External Wagering Systems.
Fantasy Contest or **Contest**	A Special Event involving any game or contest or simulation in which: • One or more players compete against each other by grouping virtual rosters of real athletes or participants belonging to professional Sports Events or Special Events. • These teams compete against each other based on cumulative statistical results of the performance of athletes or participants in real Sports Events or Special Events for a specific period. • The winning outcomes reflect the skills and relative knowledge of the players and are mostly determined by the cumulative statistical results of the performance of athletes or participants in real Sports Events or other Special Events.
File	All documents that have not been declared as subject to disclosure by a legal provision and other materials related to a specific matter that is or has been before the Commission's consideration.
Financial Instrument	Any tangible item of value tendered in wagering, including, but not limited to bills, vouchers, and winning wager tickets.
Firewall	A component of a computer system or network that is designed to block unauthorized access or traffic while still permitting outward communication.
Frames Per Second	The number of consecutive full-screen images that are displayed each second on a screen or monitor.
Generic Accounts	User accounts that are shared by multiple users (using the same password) to gain access to any component of a Sports Betting System: application, database, or operating system. User accounts established by/for and used by Technology Platform Providers of the system for Technology Platform Provider support purposes are not considered to be generic accounts.
Global Risk Management	Management, consultation, instruction, or transmission of information relating to Sports Betting by an Operator who also holds a license to conduct Sports Betting in another Permissible Jurisdiction. The term includes: • The management of risks associated with Sports Betting involving a Sports Event or Special Event for which a Wager may be accepted; • The setting or changing of Wagers, cutoff times for Wagers, acceptance or rejection of Wagers, pooling or laying off of Wagers, lines, point spreads, odds or other activity relating to Sports Betting.
Group Membership	A method of organizing user accounts into a single unit (by job position) whereby access to system functions may be modified at the unit level and the changes take effect for all user accounts assigned to the unit.

Guest	Any person or passerby for a price, use, possess or have the right or intention to use or possess any room or rooms in hotels, for a specified period.
Hosting Center	An entity hosting on its premises any part(s) of Commission regulated hardware or software of the Sports Betting System.
Identity Verification Service Provider	An entity who verifies, or provides information for the verification of, the identification of individuals.
Imprest Basis	A specific amount of funds which are replenished from time to time or at the end of a shift in exactly the value of the expenditures made from the funds as documented. A review is made by a higher authority of the propriety of the expenditures before the replenishment.
In-Play Wager	A wager that is placed while an event is in-progress or actually taking place.
Incompatible Function	A function, for accounting control purposes, that places any person or function in a position to both perpetrate and conceal errors or irregularities in the normal course of his/her duties. Anyone recording transactions and having access to assets ordinarily is in a position to perpetrate errors or irregularities. Persons may have incompatible functions if such persons are members of functions that have supervisors not independent of each other.
Incident	Any adverse event that compromises system data, system computer networks, or system security, including but not limited to loss of confidentiality of information, compromise of integrity of information, misuse of service, systems or information, denial of service, damage to systems, theft of systems or data storage components, and any other suspicious activity, event or situation related to security of information or information systems.
Independent	The separation of functions to ensure that the employee or process monitoring, reviewing, or authorizing the controlled activity, function, or transaction is separate from the employees or process performing the controlled activity, function, or transaction.
Independent Test Laboratory	Laboratory approved by the Commission to evaluate the equipment, processes and programs against the provisions of applicable law, regulation, orders and resolutions.
Individual or **Person**	Any natural or legal person, association, board, organization, partnership, or limited liability corporation, joint venture, government, estate, subsidiary, arbitrator, transferee or agent, regardless of their organizational structure or nature.
Information Security	Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability
Information Security Management System (ISMS)	A defined, documented management system that consists of a set of policies, processes, and systems to manage risks to organizational data, with the objective of ensuring acceptable levels of cybersecurity or information security risk.
Integrity Monitoring Procedures	A system of policies and procedures approved by the Commission through which the operator receives and sends reports from other operators to assist in identifying suspicious activity.
Internal Auditors	Persons who perform an Audit Function that are independent of the function subject to audit. Internal audit personnel may provide audit coverage to more than one operation within a sports betting operation.
Internal Controls	The operator's internal controls
Internet	An interconnected system of networks that connects computers around the world via TCP/IP.
Internet Betting	The business of accepting bets on any Sports Event or Special Event through the use of electronic communication and platforms such as the internet, web pages, and mobile applications including mobile platforms for Sports Betting that allow a person to use money, checks, electronic checks, electronic money transfers, micro transactions, credit cards, debit cards or any other means, to transmit information to a computer and complete the transaction with the corresponding information. Prepaid debit cards are excluded from this definition, when the origin of the funds is unknown.
Internet Protocol Address (IP Address)	A unique number for a computer that is used to determine where messages transmitted on the Internet should be delivered. The IP address is analogous to a house number for ordinary postal mail.
Involuntary Exclusion List	A list of persons who are to be excluded or ejected from a licensed operation in the territorial limits of Puerto Rico. The Involuntary Exclusion List consists of persons who have violated or conspired to violate laws related to gaming, cheats, willful tax evaders, individuals whose presence in a licensed gaming establishment would adversely affect public confidence and trust in the gaming industry, and persons whose presence in a licensed gaming establishment poses the potential of injurious threat to the interests of the territorial limits of Puerto Rico.

IT Personnel	Employees of the Operator or an IT Service Provider who are independent of the operation of sports betting; and who have been designated to perform the information technology function for the operation of critical components of the Sports Betting System. The term is not limited to employees within an IT Function.
IT Service Provider	A person or an entity engaged by the Operator to provide management, including system administration, user access administration, support, security, or contingency plan services for Commission regulated hardware or software.
Key	A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification.
Key Employee	A person who is employed by the operator in a director or function head capacity or who is empowered to make discretionary decisions that regulate Sports Betting Operations as determined by the Commission.
Key Management	Activities involving the handling of cryptographic keys and other related security parameters (e.g., passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.
Kiosk	Wagering Equipment that players use to place wagers, purchase entries, redeem winning wager tickets and/or vouchers, open accounts, make account deposits and/or withdrawals. This term is synonymous with "*Self-Service Wagering Device*" in GLI-33
Knowingly	To have known or should have known.
Label	The label that adheres to the upper left of the Kiosk cabinet screen, assigned and fixed by the Commission once it is approved for use as a Kiosk. It will have to contain electromagnetic technology, RFID, for its acronym in English.
Law	Law No. 81 of July 29, 2019, as amended, known as the Law of the Gaming Commission of the Government of Puerto Rico.
Layoff Wager	A wager placed by a Sports Betting Operator or Service Provider with another Sports Betting Operator or Service Provider for the purpose of offsetting player wagers made pursuant to these MICS.
License	Authorization granted by the Commission or the Administrator, to a natural or legal person in accordance with the rights and obligations provided by law and the Regulations.
Location Number	The number assigned to an area of the Authorized Location which identifies the site where the Wagering Equipment is positioned.
Location Service Provider (LSP)	An entity who identifies, or provides information for the identification of, the geographic location of individuals.
Log	Record of Interventions, malfunctions, claims or any other incident.
Main Bank	An area providing maximum security for the materials housed therein and for the activities performed therein within the main cage. It operates on a perpetual inventory and serves as the central location in the Authorized Location for the custody and accountability of all assets used to fund the operation. The functions of the Main Bank are as follows: • The custody of financial instruments, forms, documents, and records normally generated or utilized by main bank cashiers. • The exchange of financial instruments, for supporting documentation. • The responsibility for the overall reconciliation of documentation generated by all cage cashiers. • The receipt of financial instruments from the count rooms. • Such other functions normally associated with the operation of the main bank.
Main Bank Cashier	A cage cashier whose duties include working in and performing all the functions normally associated with a main bank.
Main Cage	A physical structure that houses the cage cashiers and serves as the central location for the following: • The custody of the cage inventory comprising financial instruments, forms, documents, and records normally associated with the operation of a cage. • Such other functions normally associated with the operation of a cage.
Malfunction	An error in the functioning of the Sports Betting System, Wagering Equipment, Mobile App, or Site including, the front-end application not being accessible to Players or the Sports Betting Operations is not working.

Meter	Mechanical, electric, or electronic device that continuously and automatically counts bills or their equivalent, including ticket entry meters, deposit meters, prize meters and similar meters related to Kiosks.
Mobile App	Any mobile application or digital platform approved by the Commission for the Sports Betting Operation over the internet.
Mobile Code	Executable code that moves from computer to computer, including both legitimate code and malicious code such as computer viruses.
Mobile Device	Any portable device, mobile phone, tablet or laptop, which is capable of connecting to or using any mobile telecommunication or Wi-Fi technology to enable or facilitate transmission of textual material, data, voice, video or multimedia services over the Internet or otherwise.
Multi-Factor Authentication	A type of strong authentication that uses two (2) of the following to verify a player's identity including, information known only to the player, such as a password, pattern or answers to challenge questions, an item possessed by a player such as an electronic token, physical token or an identification card, or a player's biometric data, such as fingerprints or facial or voice recognition.
Offset	Money that the Operator is required by to deduct from a Player's Winnings for certain debts owed to the Commonwealth, for delinquent child support obligations or as otherwise required by the applicable Laws and Rules.
Operational Day	The period from the beginning to the end of day the licensed operations, which shall not exceed twenty-four (24) hours. For twenty-four (24) hour operations, this shall be midnight to midnight.
Order or **Resolution**	Any decision or action of the Commission of particular application in which rights or obligations of one or more specific posts are awarded or in which administrative penalties or sanctions are imposed, with the exception of executive orders issued by the Governor.
Party	Any person or agency authorized by law, including the Commission, in the complaints filed by the Commission, to whom the Commission's claim is specifically directed or who is one of the parties to said litigation, or who is allowed intervene or participate in the same or that has filed a request for review or compliance with any order or is designated as a party to said procedures.
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Payment Service Provider (PSP)	An entity who directly facilitates the depositing of funds into or withdrawing of funds from Player Accounts.
Peripheral	An internal or external device connected to wagering equipment that supports credit acceptance, credit issuance, player interaction, or other specialized function(s).
Permissible Jurisdiction	Any jurisdiction in which Global Risk Management or the wagering on a Sports Event or Special Event is lawful or not otherwise expressly prohibited under the laws of that jurisdiction.
Person	Any natural or legal person, association, corporation, Commission, partnership, or limited liability Commission, joint venture, government, estate, subsidiary, arbitrator, transferee or agent, regardless of their organizational structure or nature.
Personally identifiable information (PII)	Sensitive information that could potentially be used to identify a particular player. Examples include a legal name, date of birth, place of birth, social security number (or equivalent government identification number), driver's license number, passport number, voter's Identification or other official identification, residential address, phone number, email address, debit instrument number, credit card number, bank or financial account numbers of any type with or without passwords or access code that may have been assigned, names of users and passwords or access codes to public or private information systems, tax information, or other personal information if defined by the Commission.
Personal Identification Number (PIN)	A numerical code associated with an individual and which allows secure access to a domain, account, network, system, etc.
Physical Address	For an individual, a residential or business street address; for an individual who does not have a residential or business street address, an Army Post Office, Fleet Post Office box number, the residential or business street address of next of kin, or of another contact individual.
Player Account	An account established by the operator for an individual player to engage in Sports Betting where information relative to player and financial transactions are recorded on behalf of the player including, but not limited to, deposits, withdrawals, wagers, winnings, and balance adjustments.

Player Loyalty Program	A program that provides incentives for players based on the volume of play or revenue received from a player.
Point of Sale or Satellite	An authorized location licensed as a point of sale by the Commission to accept and pay sports wagers on behalf, and as a satellite of a Principal Operator to players authorized to carry them out through a Sports Betting Administration Agreement.
Pre-Play Wager	A Wager placed prior to the start of an event.
Prepaid Access Instrument	A card, code, electronic serial number, mobile identification number, personal identification number or similar device used in conjunction with an Interactive Gaming System that allows player access to funds that have been paid in advance and can be retrieved or transferred at some point in the future through such a device.
Principal Operator	An authorized location licensed as a Principal Operator by the Commission to accept and pay sports bets to bettors authorized to carry them out. The Principal Operator may offer services to other Operators to operate as Satellites through a Sports Betting Administration Agreement
Printer	A wagering equipment peripheral that prints wager tickets and/or vouchers.
Prize	An award, incentive, promotion, or anything of monetary value, including but not limited to, cash or a cash equivalent, wagering credits, merchandise, or another wager.
Program	The intellectual property and instructions collected or compiled, included in the system and its components, including procedures and associated documentation related to the operation of a computer, a computer program or a computer network.
Programming	Configuration and instructions programmed in the system and associated equipment, including procedures and documentation related to the operation of the computer, its programs or the network.
Prohibited Sports Wager	Any sports wager not approved by the Commission or that is otherwise unauthorized under these MICS or by Regulations or Law.
Prohibited Player	Those prohibited from participation in Sports Betting, including • Any individual under the age of eighteen (18) • Any employee of the Commission • Any individual who is listed on the Commission's Voluntary Exclusion List or Involuntary Exclusion List • Any individual who is listed on any operator's Voluntary Exclusion List or Involuntary Exclusion List • The operator, a director, officer, owner, contractor, or employee of the operator, or any relative living in the same household • Any individual, group of individuals, or entity with access to confidential information or insider information held by the operator; or • Any individual, group of individuals, or entity acting as an agent or surrogate for others. • Any person or entity included in the Specially Designated Nationals and Blocked Persons List issued by OFAC
Protocol	A set of rules and conventions that specifies information exchange between devices, through a network or other media.
Proxy	An application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it. This effectively closes the straight path between the internal and external networks. Making it more difficult for an attacker to obtain internal addresses and other details of the internal network.
Puerto Rico	The Commonwealth of Puerto Rico.
Random Number Generator (RNG)	A computational or physical device, algorithm, or system designed to produce numbers in a manner indistinguishable from random selection.
Regulations	The Puerto Rico Sports Betting Regulations approved and promulgated by the authority conferred on the Puerto Rico Gaming Commission by Law No. 81 of July 29, 2019, as amended, known as the Law of the Gaming Commission of the Government of Puerto Rico.
Remote Access	Any access from outside the system or system network including any access from other networks within the same Authorized Location.
Report	Information produced by the System that is viewed via display, printed, or saved to a file depending on the needs of the Commission.
Risk	The likelihood of a threat being successful in its attack against a network or system.

Satellite Cage	A physical structure separate and apart from the main cage which is maintained on an imprest basis and may perform some of the functions of the main cage.
Satellite Surveillance Equipment	Surveillance monitors, recorders, remote selectors and other ancillary equipment located in an area other than the surveillance room and used for surveillance
Seal	Label, plate, mark or device attached or placed to identify the certification of the kiosk after being verified and approved by the Commission.
Security Policy	A document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance
Sensitive Information	Information such as confidential information, PII, wagering data, validation numbers, authentication credentials, PINs, passwords, secure seeds and keys, and other data that shall be handled in a secure manner.
Server	A running instance of software that is capable of accepting requests from clients, and the computer that executes such software. Servers operate within a Client-Server Architecture, in which "servers" are computer programs running to serve the requests of other programs ("clients").
Service Accounts	Accounts on which automated system functions are dependent to execute. A service account does not correspond to an actual person. These are often built-in accounts that an automated system function (service) uses to access resources they need to perform its activities. However, some automated services may require actual user accounts to perform certain functions and may be employed using domain accounts to run services.
Service Provider	The person or company authorized by a license issued by the Commission to offer services or any goods that are necessary for the Sports Betting Operation.
Signature	The first or initial name, the surname and the number of the license that are subject to the own person.
Site	Any website operated by the operator through which a player can access their Player Account to place wagers online.
Source Code	A text listing of commands to be compiled or assembled into an executable computer program.
Source Code Repository	A secured environment that is used to store software source code once it has been approved for introduction into the production (live) environment. The repository is secured such that developers cannot modify code once it has been stored. In this way, the repository provides a history of a given software system ordered by version.
Special Events	Any game or event that generates Sports Betting, including, but not limited to, Esports Competitions recognized by a Sports Governing Body or equivalent, Virtual Events, and Fantasy Contests and whose duration does not exceed thirty (30) days. The Commission may authorize contests and competitions, even if they are not sports, provided that the winner is determined in real time. The Commission will ensure that they provide security for all parties involved in the industry to avoid tax evasion, money laundering and any other criminal conduct typified as such in the corresponding statutes. Under this concept, bets are not authorized in Special Events designed for participants under eighteen (18) years. Sports Betting on Special Events are also not authorized from educational institutions of primary, intermediate and secondary level. This definition does not include the Traditional Lottery or the Additional or Electronic Lottery, which will be regulated by the Treasury Department.
Sports Betting	The business of accepting bets, in cash or their equivalent, in any Sports Event, Special Event, or on the individual performance of individuals who participate in a Sports Event or Special Event, or a combination of these, authorized by the Commission through a Sports Betting System. This includes, but is not limited to, all in-person communication, kiosks and self-service stations located somewhere in an authorized location, or through internet. This definition does not apply to: • Authorized bets on Act No. 83 of July 2, 1987, as amended, known as the "Horse Racing Industry and Sports Law of Puerto Rico". • All authorized games of chance in the Law No. 221 of May 15, 1948, according to amended, known as the "Law on Gambling and Machine Authorization Slots in Casinos"; and • Fantasy Contests regulated in Law No. 81 of July 29, 2019, according to an amendment, known as the Gaming Commission Act of the Government of Puerto Rico; This term is synonymous with "*Event Wagering*" in GLI-33.

Sports Betting Administration Agreement	A written agreement between a Principal Operator and a Point of Sale, for the administration and operation of an Authorized Location to operate as a Satellite of the Principal Operator.
Sports Betting Manager	A key employee of the Sports Betting Operator, or a qualified employee of a licensed Service Provider that is operating under a contract with a Sports Betting Operator, responsible for the operations of sports betting conducted pursuant to these MICS.
Sports Betting Operations	The business of accepting wagers on Sports Betting for any Sports Event or Special Event, either through the use of Wagering Equipment within an Authorized Location or through the use of electronic communication and platforms such as the internet, web pages, and mobile applications including mobile platforms for Sports Betting that allow a person to use money, checks, electronic checks, electronic money transfers, micro transactions, credit cards, debit cards or any other means, to transmit information to a computer and complete the transaction with the corresponding information. Prepaid debit cards are excluded from this definition when the origin of the funds is unknown.
Sports Betting Operator or **Operator**	An entity authorized by a license issued by the Commission to accept and pay wagers in Sports Betting, either in person within an Authorized Location or through a Mobile App or Site on the Sports Betting System, within the territorial limits of Puerto Rico, in compliance with the local and federal legal framework.
Sports Betting System	The hardware, software, firmware, communications technology, other equipment, as well as operator procedures implemented in order to allow player participation in Sports Betting, and, if supported, the corresponding equipment related to the display of the wager outcomes, and other similar information necessary to facilitate player participation. The system provides the player with the means to submit and manage wagers. The system provides the operator with the means to review player accounts, if supported, suspend events, generate various wagering/financial transaction and account reports, input outcomes for events, and set any configurable parameters. This term is synonymous with "*Event Wagering System*" in GLI-33.
Sports Event	Any professional Sports Event, athletic event, college or university sport, as well as any Sports or Athletic Event recognized by a Sports Governing Body. The term Sports Event may include, but is not limited to, other types of events or contests authorized by the Commission, as long as the winner is determined in real time. Excluded from this definition of Sports Event: • The horse racing events regulated in Law No. 83 of July 2, 1987, according to an amendment, known as the Puerto Rico Horse Racing and Equestrian Law; • The electronic lottery games, draws, or contests by virtue of Law No. 10 of May 24, 1989, according to the law, known as the Law to Authorize the Additional Lottery System; • The games, draws, or contests by virtue of Law No. 465 of May 15, 1947, as amended, known as the Lottery of Puerto Rico; and • Any prohibited or illegal Sports Event.
Sports Governing Body	The organization, league, or association that prescribes final rules and enforces codes of conduct with respect to a Sports Event or Special Event and athletes or participants therein.
State of Intoxication	A state wherein a person's speech, balance, co-ordination or behavior is noticeably affected and there are reasonable grounds for believing this state to be induced by alcohol, narcotics or any intoxicating substance.
Statistics Service Provider	An entity chosen by the operator to sell or provide information to the Sports Betting System, from among those services providing statistical data, and gather statistical data on team and individual performances, which information is used to calculate odds/payouts and prices.
Structure or **Structuring**	The process of a person engaging in a transaction or transactions, whether acting alone or in conjunction with others or on behalf of others, who conducts or attempts to conduct one or more transactions in currency, in any amount, at one or more operators on one or more days, in any manner, for the purpose of evading the reporting requirements under these MICS.
Sufficient Clarity	The capacity of a CCTV System to record images at a minimum of 20 frames per second or equivalent recording speed and at a resolution sufficient to clearly identify the intended activity, person, object, or location.
Supervisor	All supervisory personnel in the different areas of the Commission, including, but not limited to, Assistant Directors and other supervisors so designated by the director.
Supplier or **Vendor**	An individual, group of individuals or entity that seeks to sell or lease Wagering Equipment, software, systems, data or services relating to the conducting of sports betting, by an Operator or Service Provider, as determined by the Commission. The term does not include a Sports

	Governing Body or equivalent that supplies its data directly to an Operator or Service Provider.
Surveillance	The capability to observe and record activities being conducted in an Authorized Location
Suspicious Activity	Any unusual activity which cannot be explained and is indicative of match-fixing, the manipulation of an event, misuse of inside information, or other prohibited activity.
System Administrator	The individual(s) responsible for maintaining the stable operation of the Sports Betting System (including software and hardware infrastructure and application software).
Takeout or Fees	An amount retained and not distributed by the operator from the total amount of wagers on an event.
Technology Platform Provider or **Provider**	An entity authorized by a license issued by the Commission to provide the programs (software) for participation in Sports Betting, and the peripherals (hardware) where they reside.
Third-Party Service Provider	An entity who acts on behalf of the operator to provide services used for the overall conduct of Sports Betting.
Threat	Any circumstance or event with the potential to adversely impact network operations (including mission, functions, image, or reputation), assets, or individuals through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a system vulnerability.
Ticket Writer Station	Wagering equipment that at a minimum will be used by an employee for the execution or formalization of wagers placed on behalf of a player at the Authorized Location. This term is synonymous with "*POS Wagering Device*" in GLI-33.
Time Stamp	A record of the current value of the system date and time which is added to a message at the time the message is created.
Total Revenue Received	Revenue received by an Operator from players for Sports Betting in Puerto Rico for the purpose of accepting and paying wagers
Tournament or **Contest/Tournament**	An organized, measured event that permits a player to engage in competitive play against other players. An out-of-revenue tournament involves only non-wagered play using tournament credits or points that have no cash value. In contrast, an in-revenue tournament allows for wagered play in conjunction with the operation of the tournament.
Transmission Control Protocol/Internet Protocol (TCP/IP)	The suite of communications protocols used to connect hosts on the Internet.
Unauthorized Access	A person gains logical or physical access without permission to a network, system, application, data, or other resource.
Unusual Activity	Abnormal activity exhibited by players and deemed by the operator, the Commission or another governing body as a potential indicator of suspicious activity. Unusual activity may include the size of a player's wager or increased participation volume on a particular event or wager type.
User Access Administrator	The individual(s) responsible for and has system authorization/access to add, change, or delete user accounts and associated user provisioning. User provisioning consists of assigning application functions matching the employee's current job responsibilities, unless otherwise authorized by management personnel, to ensure adequate separation of duties.
Verifier	Any employee who witnesses and signs a document confirming an approved transaction as permitted in these MICS.
Version Control	The method by which an evolving approved Sports Betting System is verified to be operating in an approved state.
Video Game	An electronic game that involves interaction with a user interface to generate visual feedback on a video device such as a computer monitor.
Virtual Events	A Special Event involving simulations of sports, contests, and matches whose results are determined solely by an approved Cryptographic Random Number Generator (RNG). Virtual Events are comprised either an animated graphical representation of a real Sports Event, or a compilation of scenes corresponding to a Sports Event previously carried out.
Virtual Private Network (VPN)	A logical network that is established over an existing physical network and which typically does not include every node present on the physical network.
Virtualized or Cloud Environment	An off-site, third-party platform with a suite of applications that the organization subscribes to for services such as: Infrastructure as a Service; Platform as a Service; Software as a Service; etc.; that are required to operate its business.

Virus	A self-replicating program, typically with malicious intent, that runs and spreads by modifying other programs or files.
Voluntary Exclusion List	The list of persons who wish to refrain from participating in Sports Betting and types of gambling offered by the Commission
Voucher	The document printed with a barcode or other mechanism issued by Kiosks or Ticket Writer Stations to the player, which represents an amount of money to the bearer, which can be exchanged for cash or inserted to play the indicated credits in a Kiosk, or they can be redeemed for cash in the kiosk or in the main cage.
Vulnerability	Software, hardware, or other weaknesses in a network or system that can provide a “door” to introducing a threat.
Wager or **Bet**	Selection made by the player of the type of Sports Event or Special Event as evidenced by a receipt and / or any sum of money or representation of value that is risked on a Sports Event or Special Event whose outcome is uncertain.
Wager Ticket	A printed or virtual wager record that evidences a wager. This term is synonymous with “*Wager Record*” in GLI-33.
Wagering Equipment	A mechanical, electronic, or other device, mechanism, or other equipment, and related supplies used or consumed in the operation of sports betting at a licensed Authorized Location including, but not limited to, a Ticket Writer Station or Kiosk installed to accept sports wagers. This term is synonymous with “*Wagering Device*” in GLI-33.
Wagering Rules	Any written, graphical, and auditory information compiled by the operator for the purpose of summarizing portions of the internal controls and certain other information necessary to inform the public of the functionality of the Sports Betting Operations.
Winnings	The prize a player wins, including the amount of the wager in the course of participating in sports betting.
Withdraw or **Withdrawal**	Any request by a Player to transfer funds from the Player Account.