STADIUM LLC

Internal Controls

Contents

Contents 1
Introduction 6
Key Definitions 6
AML/BSA Terminology 6
Betting Terminology 7
Governance Terminology 9
Technology Terminology 10
Account Terminology 10
Third Party Services Terminology 11
Internal Controls 11
Overview 11
Changes to Internal Controls 11
Organization Structure Controls 13
Segregation of Duties 13
Organizational Structure 13
Executive Leadership & Management: Roles and Responsibilities 14
Accounting Function 15
Internal Audit Function 15
Sports Betting Function 16
Compliance Function 17
Information Technology (IT) Function 18
Security Function 19
Surveillance Function 20
Main Cage Function 21
Job Descriptions – Roles and Responsibilities 22
Staff Training 23
Background Checks 24
External Consultants 24
Controls: Systems and Components Used for Sports Betting 26
Initial Certification 26
Change Management Program (CMP) 26
Annual Re-Certification 27

Security of Sports betting systems 28
System Integrity and Security Audit 28
Sports Betting Asset Management 29
Asset Disposal 31
System Architecture 31
Physical and Environmental Security 31
Communications Security 34
Encryption and Cryptographic Controls 35
Firewalls 37
Third-Party Systems 37
Information Security Management System (ISMS) 38
ISMS Plan 38
ISMS Security Officer 39
ISMS Audit 39
ISMS Risk Management and Assessment 40
ISMS Incident Management Procedures 41
Controls: Maintenance of Sports betting systems 42
Monitoring of Critical Services and Critical Components 42
Logging 46
Exception Reports 46
Requirements for System Verification 50
Control Program Verification Listing ("CPVL") 51
System Procedures 52
Procedures for Maintenance 53
User Access Controls 53
Access Control Policy 53
Provisioning of Access Privileges 54
Logical Access Control 58
User Access Functions 59
Removal of Access Privileges 61
Generic Accounts 62
Service Accounts 63

Default Accounts 63
Test Accounts 64
List of Accounts 65
User Access List 66
User Access Logging 68
Control 44: Remote Access to the Sports Betting System 68
Software Downloads 70
Backup and Recovery Procedures 71
Contingency Plan 71
General Operating Procedures 72
Protection of Unpaid Funds 72
Responsible Play 75
Prevent Extension of Credit or Promotion 76
Authorized Sports Betting 76
Wagers on Sports Events and Special Events 76
Wagering Periods 79
Placement of Wagers 79
Pre-Play Wagering 80
In-Play Wagering 80
Placing a Bet 80
Ticket Writer Stations 81
Bet acceptance 81
Wager Cancellations and Voids 81
Timing for Bet Acceptance or Voids 84
Procedures for Mobile Account Wagering 85
Placing a bet through the mobile app 85
Winning Wager Ticket and Voucher Payment 86
Payment of Winnings 86
Checkout Standards 87
Redemption during System Failure 87
Lost Wager Tickets and Vouchers 90
Payout Process for Mail-In Winning Wager Tickets and Vouchers 90

Contests/Tournaments, Bonuses and Promotions, and Player Loyalty Programs 91
Bonus or Promotional Payouts, Drawings and Giveaway Programs 92
Player Loyalty Programs 93
Complimentary Services or Items 94
Contests and Tournaments 95
Sports Betting Risks and Controls 97
Events, Odds and Result Management 97
Monitoring Activities and Reporting Fraud and Suspicious Conduct 97
Location Service Providers 101
Authorized Location 102
Hours of Operation 102
Betting Counters and Windows 102
Main Cage 103
Account Controls for a Main Cage 103
Employee Segregation of Duties 105
Cage Access 107
Cage Accountability 107
Ticket Writer Station Reconciliation of Assets and Documents 108
Kiosks 110
Kiosks Identification 110
Kiosks Restrictions 111
Access to Kiosks 111
Kiosk Cash Storage Box 111
Collecting Currency Cassettes and Cash Storage Boxes from Kiosks 111
Kiosk Count and Documentation 113
Kiosk Replenishment 114
Kiosk Reconciliation of Assets and Documents 115
Count Room Access and Count Team 115
Wagering Equipment 116
Certification 116
Time & Date 116
ADA Compliance 117

Shipping and Receiving Equipment 117
Location and Security 118
Installation 119
Maintenance 119
Malfunctions 120
Removal, Retirement and/or Destruction 120
Communications Technology 122
Key Controls 122
Security and Surveillance 124
Authorized Location Security 124
Identification Badges 124
Policy on Personnel Protection 124
Prevent Wagering by Prohibited Players or Intoxicated and Impaired Persons 125
Closed Circuit Television (CCTV) Systems 125
Power Outages 127
Player Account Management 127
Player Account Procedures 127
Registration and Verification of Players 128
Protection of Player Accounts 131
Personally Identifiable Information (PII) Security 132
Payment Service Providers 135
Player Funds Maintenance 135
Player Funds Protection 135
Financial Transactions 135
Deposits 138
Withdrawals 139
Electronic Funds Transfers (EFT) 140
Adjustments 141
Account Closure 141
Dormant and Closed Accounts 142
Reports and Information Storage 142
Reporting Requirements 142

Exception Reports 144
Electronic Storage of Information 146
Bank Secrecy Act (BSA) Compliance 147
Transactions in Excess of $10,000 147
Anti-Money Laundering (AML) Compliance 151
AML Compliance Policy 151
AML Risk Assessment 152
AML Compliance Manager 153
AML Program Violation 154
Accounting and Auditing Procedures 154
Accounting Controls 154
Internal Audit Program 154

Introduction

The Stadium LLC, doing business as WinIn ("Stadium," "WinIn," or the "Company") adopts the following Internal Controls (the "ICs") pursuant to Act No. 81 of 2019, known as the Law of the Gaming Commission of the Government of Puerto Rico ("Law"), and Article 3 of the Puerto Rico Sports Betting Regulations, Regulation No. 9316 of October 21, 2021 ("Regulations"). These ICs are also compliant with the Minimum Internal Controls Standards adopted by the Puerto Rico Gaming Commission (the "Commission").

The following procedures provide a baseline for conducting Know Your Customer ("KYC") reviews, Anti-Money Laundering ("AML") Investigations and OFAC Sanctions reviews. These procedures should be used in conjunction with the AML Policy and all applicable internal applications.

Key Definitions

The following definitions are not all-inclusive of all pertinent definitions applicable to these procedures. Definitions are broken down further into categories, but the list is not all-inclusive:

AML/BSA Terminology

a) *Anti-Money Laundering ("AML")* – the legal controls that require financial institutions and other regulated entities to prevent, detect and report money-laundering activities.

b) 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.

c) *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.

Betting Terminology

a) Athlete or Participant – individual, team, or other entity whom a player selects for the purposes of a wager in sports betting.

b) *Authorized Player or Player* – individual, 18 years of age or older, whose identity was authenticated and recorded through a means implemented by the operator.

c) College or University Sports Event –offered or sponsored by or played in connection with a public or private institution offering higher education services.

d) *eSports Competition* – a Special Event involving the competitive playing of video games between individual competitors.

e) Event – occurrence related to Sports Events and Special Events approved by the Commission.

f) *In-Play Wager* – a wager that is placed while an event is in-progress or actually taking place.

g) 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.

h) *Internet Betting Operator* – an entity authorized by a license issued by the Commission to accept and pay wagers on Sports Events or Special Events 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.

i) 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.

j) *Principal Operator* – an authorized location licensed as a Principal Operator by the Commission to accept and pay wagers to players authorized to carry them out.

k) Prohibited Player – any one of the following: (i) any individual under the age of 18; (ii) any employee of the Commission; (iii) any natural or juridical person who is listed on the Commission's, or any Operator's, Voluntary Exclusion List or Involuntary Exclusion List; For each operator, with exceptions for private pools, where their association with the operator is clearly disclosed; Any individual, group of individuals, or entity acting as an agent or surrogate for others.

l) *Special Event* – any game or event that generates sports bets, including, but not limited to, eSports and Fantasy Games, the duration of which do not exceed thirty (30) days; provided that betting on Special Events designed for players under the age of eighteen (18) or Special Events held by educational institutions at elementary, middle, and high-school level is not authorized.

m) 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: (i) authorized bets on Act No. 83 of July 2, 1987, as amended, known as the "Horse Racing Industry and Sports Law of Puerto Rico"; (ii) 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 (iii) Fantasy Contests regulated in the Law. This term is synonymous with "Event Wagering" in GLI-33.

n) *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: Horse racing events; Electronic lottery games, draws, or contests; any prohibited or illegal Sports Event.

o) Virtual Events — a Special Event involving simulations of sports, contests, and matches whose results arc determined solely by a Random Number Generator (RNG). Virtual Events are comprised either of an animated graphical representation of a real Sports Event, or a compilation of scenes corresponding to a Sports Event previously carried out.

p) *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.

q) House 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.

r) *Winnings* — the prize a player wins, including the amount of the wager in the course of participating in Sports Betting.

Governance Terminology

a) Commission or Puerto Rico Gaming Commission (PRGC) — the Puerto Rico Gaming Commission created pursuant to the Law.

b) *Employee License* — the required authorization issued by the Commission to the operator's employee in order to be able to conduct the duties of an operator.

c) Good Conduct Certificate — a document issued by the Puerto Rico Police Department that includes serious or less serious crimes for which a person has been found guilty. It also includes the sentence imposed and whether it has been served or not. Negative certificates are issued to those individuals who have not been convicted of committing any crimes.

d) *Involuntary Exclusion List* — a list of persons who are to be excluded or rejected from a licensed operation in the territorial limits of Puerto Rico. Consists of persons who have violated or conspired to violate laws related to gaming, cheats, willful tax evaders, and it includes any person or entity included in the Specially Designated Nationals and Blocked Persons List issued by OFAC.

e) 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.

f) *Voluntary Exclusion List* – list of persons who wish to refrain from participating in Sports Betting and types of gambling offered by the Commission.

TECHNOLOGY TERMINOLOGY

a) Authentication –verifying the identity of a user, process, software package, or device

b) *Geolocation* – identifying the true geographic location of an internet connection or mobile device.

c) Mobile App – any mobile application or digital platform approved by the Commission for the Sports Betting operation over the internet.

d) *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.

e) Random Number *Generator* – a computational or physical device, algorithm, or system designed to produce numbers in a manner indistinguishable from random selection.

f) 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.

ACCOUNT TERMINOLOGY

- *Deposit* – money a player adds to their Player account and may be used to place wagers.
- Dormant Account – a Player account which has had no player-initiated activity for a period of 3 years.
- *Segregated Account* – a financial account that segregates funds that are owned by players and that, by its terms, is restricted to funds owned by players in the United States, such that the operator's operational funds may not be commingled.

- Takeout or Fees – an amount retained and not distributed by the operator from the total amount of wagers on an event.

Third Party Services Terminology

- Identity Verification Service Provider – an entity who verifies, or provides information for the verification of individuals.
- *Payment Service Provider ("PSP")* – an entity who directly facilitates the depositing of funds into or withdrawing of funds from player accounts.
- 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.
- *Third-Party Service Provider* – an entity who acts on behalf of the operator to provide services used for the overall conduct of Sports Betting.

Internal Controls

Overview

Stadium maintains a robust set of internal controls that complies with the "Standards for Internal Controls" defined by the Regulations, as well as the Minimum Internal Control Standards ("MICS"). The internal controls contain narrative representations that are utilized by Stadium. The purpose of these ICs is to ensure that WinIn's sports betting operations are conducted with the appropriate operating and security controls to maintain uniform, sound, and efficient operations and to ensure that players are not exposed to unnecessary risk when choosing to participate in our sports betting services.

Stadium has designated an individual that is responsible for internal control submissions, including the coordination of communications between the Commission and Stadium. Stadium will provide the Commission a written statement signed by the Chief Financial Officer and the Chief Executive Officer attesting that the system satisfies the Regulations and MICS.

Changes to Internal Controls

Stadium shall submit to the Commission any proposed changes to its previously approved internal controls at least thirty (30) days before the change takes effect.

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

- All added text must be underlined. All deleted text must be lined out.
- Changes 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.
- Whenever changes to job titles are made, a summary of the old position, new position and reason for the change is provided under separate cover with the submission.
- Stadium maintains a log of all internal control changes. The log includes the page number(s), revision date, effective date and internal controls revision number.
- When moving text, the location of the old text is lined out and its new location noted. Any revision to the moved text must be redlined in the new location.
- Stadium will not change their internal controls until approved by the Commission.
- Emergency changes may be submitted at any time. The Commission will review emergency submissions upon receipt and returned to Stadium if they do not constitute an emergency.
- 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.
- Stadium makes available a current version of its Commission-approved internal control, and all retired representations of internal controls for a minimum of 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.
- Internal categories are defined into the following five (5) levels:
    - Substantive: affects the method of complying with the MICS.
    - Administrative: editorial, clarifies procedures or changes position descriptions or titles.
    - Deviation: constitutes an exception to or variance from the MICS. A detailed explanation of the necessity to deviate from the MICS and the compensating controls is included with the submission.
    - Emergency: 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.

- Audit Finding/Recommendation: 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.

Organization Structure Controls

Segregation of Duties

Stadium adheres to the segregation of duties to ensure proper controls of critical processes that could impact the integrity of sports betting, and to ensure that no group has overall control in a way that could impact sports betting integrity without management oversight. Stadium sets work responsibilities in order to minimize errors, limit liabilities, and increase the amount of separation between related duties. Stadium ensures 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.

Organizational Structure

Stadium maintains an organizational structure that is designed to preserve the integrity of the sports betting operation. Stadium considers the following criteria in creating and updating the organizational chart:

- Supervisory and chain-of-command for proper accountability.
- Segregation of duties 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 duties.
- Areas of responsibility which are not so extensive as to be impractical for one person to monitor.

Stadium hires and trains personnel that have the appropriate knowledge and skill, as well as, holding the appropriate license required. Supervision is provided as needed for each function by a supervisor with authority equal to as or greater than those being supervised. Each of these functions and supervisors are required to cooperate with, yet perform independently of, all other functions.

Executive Leadership & Management: Roles and Responsibilities

Stadium maintains the following positions within its executive leadership and management:

- Chief Executive Officer (CEO): Responsible for the overall success of the Company and for making top-level managerial decisions. Holds ultimate authority in making final decisions.
- Chief Financial Officer (CFO): Responsible for leading the development and execution of long-term strategies, with the goal of increasing shareholder value.
- Chief Operating Officer (COO) & General Counsel: Responsible for overseeing the day-to-day administrative and operational functions of the Company. Reports directly to the chief executive officer (CEO). As general counsel, responsible for providing expert and strategic legal advice to management. Reports to the CEO, supervises all operations managers and most service providers.
- Chief Marketing & Sales Officer: Responsible for planning, developing, implementing, and monitoring the Company's marketing strategy. His main function is to assist the Company in increasing its revenues by creating a marketing plan that gives it a competitive advantage. Reports to the CEO and supervises the advertising and products manager.
- Internal Auditor (Outsourced): Responsible for auditing compliance with the Wagering Procedures and Practices of GLI-33, these Internal Controls, as well as to the Law and Regulations of 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 noncompliance 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.

  Additionally, responsible for properly documenting the work performed, the conclusions reached, and the resolution of all exceptions. Responsible for retaining resulting working papers and documentation for a minimum of five

years.

Reports to the CEO and collaborates with the COO and Compliance Manager.

Accounting Function

Stadium maintains an accounting function that is independent from the Sports Betting Function. The Accounting Function maintains the following responsibilities:

- Oversight of accounting controls
- Preparation and control of records and data
- Control of stored data and review of documents used in operations.
- Preparation of daily financial reports
- Reconciliation of accounts with Payment Service Providers (PSPs).
- Daily audit of the sports betting documentation, a daily audit of the cage accountability, document control and signature verification.

The Accounting Manager reports primarily to the CFO and secondarily to the COO.

Internal Audit Function

Stadium maintains an Internal Audit function through a third-party service provider. The function consists of auditors that are independent of the areas subject to audit. It is supervised by personnel that have an occupational license and report to Stadium audit committee or other independent function.

The function is responsible for auditing compliance with all applicable rules and regulations, Commission feedback and internal controls, including ensuring the following:

- Proper documentation of work performed, conclusions reached, and resolution of all exceptions.
- Review and appraise the adequacy of internal controls.
- Compliance with internal controls through observations, interviews and review of appropriate documentation.
- Report instances of non-compliance
- Report any material weaknesses, and remedial recommendations, to appropriate management

Customer Service Function

The Operator shall maintain a Customer Service Function which shall be located at Stadium's principal office, if not available at each of the Authorized Locations.

The Customer Service Function shall be supervised by an employee holding an occupational license reporting to Stadium's senior management.

The Customer Service Function shall be responsible for, without limitation, the following matters:

- Assisting players with account inquiries;
- Assisting players with technical difficulties connecting to or wagering on the Sports Betting System; and
- Registering and trying to resolve player complaints and disputes.

Finally, 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.

Sports Betting Function

Stadium maintains a Sports Betting Function responsible for the conduct of sports betting in accordance with the established House Rules, laws, and regulations. It is supervised by an employee holding an occupational license endorsed with the position of Retail and Operations Manager that is employed Stadium. The Function verifies that all wagering rules and disclaimers are displayed at all times, or made readily available to the player upon request.

Each Authorized Location has a Retail and Operations Manager present at all times when sports betting is taking place. The Retail and Operations Manager is responsible for the conduct of sports betting in accordance with the established betting house rules, laws, regulations, and these Internal Controls, as well as responsible for verifying and ensuring that all betting rules and disclaimers are displayed, at all times, or made readily available to the player upon request. Additionally, the Retail and Operations Manager ensures that

there is sufficient supervision, knowledge, and training within the function to provide for the proper, responsible, and fair conduct of sports betting. The Manager is responsible for the operations of sports betting and final approval of all odds established on any wager made pursuant to laws and regulations. The Retail and Operations Manager will immediately notify the Commission upon the detection of any person participating in sports betting who is:

- Being engaged in, or attempting to engage in, or reasonably suspected of, or in the process of cheating, theft, embezzlement, collusion, money laundering, or any other illegal activity;
- Involuntarily excluded (see list); or
- Voluntarily excluded (see list).

Compliance Function

Stadium maintains a Compliance function that is responsible for ensuring Stadium's ongoing compliance with the laws and regulations, approved internal controls, changes to the control environment and interacting with the Commission regarding regulatory matters. The function is supervised by an employee holding an occupational license endorsed with the position of Compliance Manager. The Compliance Manager is responsible for:

- Monitoring audits and reviewing reports on compliance with the laws, regulations and internal controls.
- Coordinate operations with the Commission where approvals and certifications are required
- Act as custodian over internal controls and operations methods
- Coordinate all amendments of approvals processed by the Commission
- Oversee both internal and external audit disciplines

The Compliance Manager is responsible for maintaining the current status of all lists and disclosures addressed in the rules and regulations, including:

- Key Employee certifications

- Communicating with the Commission including, but not limited to, any material changes to the ownership or organizational structure, compliance failures, remedial efforts of previous Commission findings and observations, etc.

Information Technology (IT) Function

Stadium maintains an IT function that is supervised by an employee holding an occupational license endorsed with the position of IT Director. The IT Director is independent of the operation of the sports betting activity. The IT Director is responsible for the following activities:

- The quality, reliability and accuracy of all computer systems used in conducting sports betting operations, including the specifications of appropriate computer software and hardware.
- Procedures for security, physical integrity, contingency, and maintenance of:
    - Access codes and other data-related security controls
    - Electronic storage media containing data relevant to sports betting operations
    - Computer hardware, communications equipment and software used in the conduct of sports betting operations; and
    - Adequate backup and recovery procedures.
- Acquisition, installation and maintenance of all hardware, software and data communications resources required to support sports betting operations;
- Provision of physical and environment security
- Timely back-up of information resources and the development of a contingency plan
- 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
- Maintenance of IT audit procedures and the preservation of audit data
- Maintenance of current network topology, deployment of server(s) housing application and database, and inventory of software and hardware.

IT personnel will not have access to Sports Betting Systems nor signatory authority over financial instruments and payout forms, and is independent of and restricted from access to financial instruments; accounting, audit, and ledger entries; and payout forms.

Security Function

Stadium maintains a Security function that establishes and implements a security strategy in accordance with the overall operation. The personnel of the Security function who participate in any aspect of the sports betting operation are hired through a third-party agreement for which the Commission has issued a waiver.

The function is independent of the IT function with regard to the management of security risk and all aspects of the operation of Sports Betting. The function maintains access to all necessary resources to enable the adequate assessment, management, and reduction of risk.

The function is responsible for the security of the Authorized Location in all its aspects, including, but not limited to, the following:

- Collaboration with law enforcement
- Physical safety of players and employees in the Authorized Location.
- Physical safeguarding of assets transported to/from/through the Authorized Location and immediate notification to the Commission of any incident that has compromised the safeguarding of assets.
- Protection of the players, employees and Authorized Location property from illegal activity.
- Investigation of any person engaging in, or suspected of having engaged in, any potential illegal. Activities and notifying the Puerto Rico Police Department and the Commission of such investigation.
- If required by the Commission, control and maintenance of a system for the issuance of temporary credentials and authentication of such credentials.
- Review of all processes regarding security of Stadium, including the protection of information, communications, physical infrastructure, and wagering processes.

- Ensures Authorized Location(s) are secure during normal operations and during any emergencies that arise.
- Identify, monitor and remove any person who is under the age of 18 years, intoxicated or impaired, and/or involuntarily/voluntarily excluded.

The function is responsible for recording the following in a security incident log:

- Any unusual occurrences including the date, time, nature, resolution, persons involved, and the assigned Security Personnel involved in the incident.
- Review and analysis of reports of unusual activity for evidence of fraud, collusion and cheating.
- Immediate notification of appropriate supervisors and the Commission upon detecting cheating, theft, embezzlement, or other illegal activities; and
- Acting as a "verifier" when required.

The function works with the other functions to implement any security action plans. They are involved in reviewing all tasks and processes that are necessary to ensure the security of Stadium, including, the protection of information and data, communications, physical, virtual, personnel, and overall operational security. The function is supervised by an employee holding an occupational license endorsed with the position of Head of Security.

Surveillance Function

Stadium maintains a Surveillance Function for each Authorized Location which is independent of all aspects of the operation of Sports Betting. The personnel of the function are employees of Stadium. Stadium does not outsource the Surveillance function to any third-party service provider. The Surveillance personnel are segregated and independent of all other personnel for the sports betting operation.

The Surveillance Personnel shall have prior approval of the Commission before transferring into a position that is not in the Surveillance Function. In compliance with the MICS, the reverse applies as well, and any Stadium personnel being transferred into the Surveillance Function shall be previously approved by the Commission.

Surveillance personnel are trained in the use of the Closed-Circuit TV ("CCTV") System. The function is supervised by an employee holding an occupational license who reports to appropriate senior management. They are responsible for the overall surveillance of the Authorized Location including:

- Sole control of all surveillance cameras,
- Surveillance of the conduct and operation of the Kiosks, Ticket Writer Stations, and main cage.
- Movement of cash or equivalent, player checks, winning wager tickets and vouchers, and any other Authorized Location assets.
- Audio-video recording of activities in the count room;
- Detection of any person under the age of 18 years, intoxicated or impaired, and/or involuntarily or voluntarily excluded.
- Detection of cheating, theft, embezzlement, and other illegal activities in the Authorized Location.
- Video recording of illegal, suspicious and unusual activities.
- Immediate notification to appropriate supervisors and the Commission upon the detection and recording of cheating, theft, embezzlement, or other illegal activities.

During non-operational hours, Stadium shall utilize a silent alarm system and the authorized third-party security provider will provide assistance to respond to any security situations.

Main Cage Function

Stadium maintains a Main Cage ("Cage") function for each Authorized Location which is separated into independent operations for Sports Betting and other activities. The Cage is supervised by an employee holding an occupational license endorsed with the position of Cage Supervisor and reports to appropriate senior management. The Cage is responsible for:

- Custody of cash or its equivalent, player checks, winning wager tickets and vouchers, and documents and records normally associated with the operation of the Cage;
- Approval, exchange, and redemption of player checks received for the purposes of sports betting;
- Control and supervision of all Cages, ticket writers, cashiers, and the count room;

The Main Cage function must be independent of the count in respect of revenues from the Wagering Equipment.

Job Descriptions – Roles and Responsibilities

Stadium maintains a documented organizational structure, including job responsibilities that provide job descriptions for each supervisory and Key Employee position. This includes:

- Role/objectives of the position;
- Reporting relationships both internally and externally, including immediate supervisor;
- Primary duties, controls and responsibilities;
- Titles/functions
- Access to sensitive assets and areas;
- Signatory ability, including alternate procedures in cases in which the required signatory is unable to perform their duty; and
- Knowledge, skills, qualifications and experience required for the position.

As these roles form a critical part of the control environment, Stadium will 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.

Stadium 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.

Stadium may assign a lower ranked position may be assigned the job duties of a higher ranked position within the same function for the operational day, provided that the assigned position is within the same Commission Occupational License Badge Level. Personnel temporarily working in the higher ranked position will not perform verification of his/her own work. Once assigned to the higher ranked position, the personnel will not return to his/her lower ranked position for the remainder of the operational day. If personnel are promoted to a key position in Stadium, they will undergo a higher level of due diligence.

Staff Training

New hires will undergo an onboarding program, and subsequently an annual review/refresher training program, where they will be briefed on these Internal Controls and will receive specific training on the internal controls that are relevant to their individual functions. New hire onboarding will be conducted within the first month of commencing work and before interaction with a player.

Stadium conducts on-the-job training that enables all employees to be knowledgeable of all activities relating to their functions. Stadium trains on the following topics:

- Code of conduct;
- Anti-money laundering;
- 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;
- Player verification and identification recognition;
- Fraud and security awareness; and
- Regulatory controls to which the organization is subject.

In addition to the above, employees interacting directly with players are 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. As part of the training, employee knowledge of responsible play is tested. Such testing may include written questions or the interpretation of scenarios in which the employee must show he can take action in accordance with Stadium's responsible play guidelines.

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.

Training program information made available to the Commission includes, but is not limited to, the following:

- Timeframe within which new employees are required to have completed the training;
- Personnel responsible for delivering the training;
- Frequency of the training;
- Role specific training; and
- Assessment of the effectiveness of the training.

Stadium maintains records of all internal and third party provided training completed by employees. Records include name of attendees, training topics, date of the training, and results of training. Training records are kept for a minimum of five years.

Background Checks

Stadium conducts background checks on newly hired employees and annual background checks on all existing employees that are engaged in activities related to the conduct of Sports Betting. Background checks 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.

Personnel Security

Stadium has a policy and process for establishing trust in individuals that could impact the integrity of sports betting through security vetting. Additionally, it has 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 balance an individual's right to privacy with the obligation of the operator to protect the integrity of sports betting and are attached hereto as an exhibit.

External Consultants

Stadium employs external consultants from time-to-time to complete various tasks related to Sports Betting. Stadium maintains records that include the identification of the role within the business, and the nature of their contractual relationship with the business, where their ongoing involvement is critical to the business. Due diligence

conducted on the external consultants and vendors is documented and updated on an annual basis.

Code of Conduct

Stadium has a code of conduct and strives to effectively implement it.

Such code of conduct is delivered to all employees when initially employed and all employees shall formally acknowledge acceptance of this code.

As required by the Commission's MICS, the code of conduct shall include statements regarding the following:

- All policies and procedures are adhered to and that infringement or other breaches of the code could lead to disciplinary action;
- Employees are required to declare conflicts of interest on employment as and when they occur, including specific examples of conflict of interest;
- Anti-graft provisions including hospitality and gifts provided by, or given to, persons or entities with which Stadium transacts business.

Signature Requirements

As defined in the Commission's MICS, a "signature" on a document provides evidence of the person's involvement and/or authorization of the intentions reflected in the MICS. A signature is typically in the form of a stylized script associated with a person, which may include the first letter of the person's first name along with the person's full last name. However, as established by the MICS, Stadium recognizes that the "initials" of the person would not meet the requirement of a "signature".

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.

Controls: Systems and Components Used for Sports Betting

Initial Certification

Stadium, through its Compliance Manager, ensures that all products and services that they provide, as well as their Sports Betting System components deployed within the Commonwealth, are certified by an independent testing laboratory in accordance to the standards set forth in GLI-33, these Internal Controls, as well as in applicable laws and regulations. Such system components shall be accompanied by a formal certification document noting as such.

Change Management Program (CMP)

The Compliance Manager must ensure that Stadium's CMP has been developed in accordance with the most current version of the Gaming Labs International ("GLI") Change Management Program Guide as posted on the GLI website at www.gaminglabs.com. Additionally, the Compliance Manager must ensure that the program is approved by the Commission prior to implementation and audited annually by the independent laboratory. The CMP includes policies for identifying criticality of updates and submission of updates to an independent test laboratory for evaluation, which covers:

- 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.
- Documentation of 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 the documentation.
- 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.
- Processes for requests of new software or software changes which is reviewed by IT management

- Approvals to begin work on the program are to be documented
- Patching policies agreed upon with the Commission, whether developed and supported by the Operator or by the Technology Platform Provider.

The Compliance Manager must submit quarterly reports 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.

The scope of the review consists of examining a sample of changes made during the prior period to determine whether:

- the changes were properly approved at the testing and deployment stages;
- the changes were adequately documented and classified;
- the changes were properly tested, issues resolved; and
- rollback procedures applied as needed.

The evidence of the review must be maintained by the Compliance Manager and include at a minimum:

- the date and time of the review,
- the name of the independent test laboratory who performed the review,
- the changes reviewed; and
- any exceptions noted and any related follow-up on the noted exceptions.

A formal report must be produced by the evaluating independent test laboratory noting the review as complete.

Annual Re-Certification

The Compliance Manager must ensure that at least once annually, each product operating under a CMP is fully certified to the standards set forth in GLI-33, these Internal Controls, 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.

Security of Sports betting systems

Technical Security Controls

IGT, as Stadium's Technology Platform Provider, has adopted, and shall implement and maintain technical security controls that meet or exceed the Technical Security Controls of GLI-33, the MICS, the Law and the Regulations. These controls have been incorporated into Stadium's internal controls and shall be submitted to the Commission for approval.

System Integrity and Security Audit

Stadium contracts with an independent professional organization that has been approved by the Commission to perform an annual system integrity and security risk assessment of the Sports betting system.

The Compliance Manager must ensure that system integrity and security risk assessment covers all applications that transfer, store or process personally identifiable information (PII) or sensitive information, the underlying operating system, network components, and hardware changes not included in the evaluation of the re baselined Sports Betting System.

The Compliance Manager must coordinate with WinIn's technology platform provider to ensure all critical components are audited.

The Compliance Manager must ensure that the system integrity and security risk assessment on the production environment guarantees that no vulnerabilities putting at risk the security and operation of the Sports Betting System exist.

The risk assessment will be conducted under the following scope and approach:

- A review of the operational processes that are critical to compliance, specifically those in which the Sports Betting System is used.
- Performance of the vulnerability assessment and penetration testing will be performed as follows:
    - The vulnerability assessment and penetration tests will be conducted through a third party to ensure independence.
    - The vulnerability assessment will include all assets deployed in Puerto Rico.
    - The penetration test will be conducted for all assets and services published to the internet.

- The Information Systems Officer must review the firewall rules on all the perimeter and internal firewalls to ensure that the configuration and rule sets are consistent with Technology Platform Provider recommendations as well as WinIn's policies and procedures, standards, and internal controls.
- The Compliance Manager must communicate the results of system integrity and security risk assessment to the Commission no later than one month after the date of the tests. The communication must include the following:
    - The results of the operational process review
    - The assessment results issued by any third parties or service providers.
    - A statement on the results of the firewall review and any actions taken to address any findings.
    - A high-level work plan to address any findings in the operational process review or assessment reviews.
- The Compliance Manager must lead and coordinate activities associated with addressing the findings and recommendations resulting from any of the components of the system integrity and security risk assessment under the following approach:
    - The system integrity and security risk assessment will be presented to WinIn's Executive Committee to establish the priorities in terms of the risks to be addressed and ensure that the necessary resources are assigned.
    - The Executive Committee must adopt a risk treatment for each of the risks identified as a result of the system integrity and security risk assessment.
    - The Compliance Manager must ensure that the activities necessary to support the risk treatments are undertaken by their assignees.
    - The Compliance Manager must issue monthly reports to the Executive Committee as to the progress of risk management activities.
    - The Compliance Manager must issue quarterly reports to the Commission as to the progress of risk management activities.

Sports Betting Asset Management

Stadium maintains a Critical Asset Registry (CAR) that describes all critical components of the Sports betting system, including hardware and software, that impact the functionality of

the Sports betting system, or has an influence on sensitive information is stored/handled by the system.

The current Critical Asset Registry (CAR) is as follows:

Component	Description	Provider or Vendor
SportsPlay Platform	The core processing unit of the Sports Betting System.	International Game Technology PLC ("IGT")
SportsPlay Player Account Management	The software component used by players to manage their bets.	IGT
Sports Betting Kiosks	Free-standing hardware units in which players can place bets.	IGT
World Till	The hardware and software components deployed at authorized locations to handle player service requests.	IGT
Local Networking Equipment	The networking equipment that interconnects all hardware and software components deployed locally at authorized locations.	WorldNet
Wide Area Network	Virtual private network (VPN) that connects the authorized locations to the SportsPlay Platform.	WorldNet

Stadium ensures 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.

Asset Disposal

Stadium disposes of assets securely and safely using sound practices. Prior to disposal or re-use, assets containing storage media are investigated and checked by the Information Systems Officer, or its designee, to ensure that any licensed software, as well as sensitive information has been removed or securely overwritten (i.e., not just deleted). A record of the disposal of equipment or media is maintained by Stadium.

System Architecture

Stadium, through its Information Systems Officer, develops and maintains documentation of the overall Sports Betting System architecture, including security measures, to ensure the integrity of the secured storage and processing of data. All security domains, points of access, and communication media for sports betting operations are documented. Production networks serving the Sports Betting System and its critical components are segregated into security domains based on a risk assessment of the functions performed on each network. The risk assessment contains and considers the following:

- Devices and software deployed on each WinIn network (e.g., wireless devices, database servers, networking devices, remote desktop capabilities).
- Accessibility of the network from the public Internet.
- Value and classification of the information stored or processed in the network.
- Access control policy and access requirements for the applications on the network.

Boundaries between networks having different security domains are secured from outside traffic. WinIn's systems are configured to detect and report security-related events at security domain boundaries.

Stadium provides a layered approach to security within the production environment to ensure secure storage and processing of data. The architecture supports the use of layered access controls to applications running on the network.

Physical and Environmental Security

Stadium's production datacenters, computer rooms, network operations centers, and other defined critical locations housing critical components of the Sports betting system are maintained by Continent8 Technologies, which is an independent third-party licensed by the

Commission to provide data hosting services to IGT, Stadium's Sports Betting System's platform provider. These are located at 316 Avenida de la Constitución in San Juan, Puerto Rico.

If there are any changes to the locations where Sports Betting System components or any associated staff are deployed, Stadium's Compliance Officer shall notify the Commission.

For any locations housing critical components of the Sports Betting System, Netwave's internal controls and procedures for monitoring data centers, which are adopted by Continent8 as data hosting tenant in such facilities and which attached to these Internal Controls, are implemented and documented, including delineation of the methods, processes and practices used in meeting the following at a minimum:

- Redundant power sources to reduce the risk of data loss in case of interruption of power.
- Adequate climate control and fire suppression equipment.
- Security mechanisms, such as traditional key locks, biometrics, and combination door lock, or electronic key card system to prevent unauthorized physical access to areas housing critical components of the Sports Betting System.

A Power Distribution Diagram for Netwave's Data Center Room B showing the above for Continent8's area and consumption is also attached to these Internal Controls.

Physical access to the locations housing critical components of the Sports Betting System is restricted, secured, and monitored by Stadium's external providers, which are licensed by the Commission. In compliance with the MICS, such access requires multi-factor authentication.

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

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. Certain non-IT personnel, including the Technology Platform Providers of the Sports Betting System's computer equipment, are allowed access to the locations Sports betting system only when authorized and accompanied and continuously monitored 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. A

record of each access by non-IT personnel is maintained and includes the name of the visitor(s), time and date of arrival and departure, purpose of the visit; and the name of IT personnel authorizing the access.

The locations housing critical components of the Sports Betting System are remotely located outside of the authorized location at a hosting center licensed by the Commission, with each location selected having adequate security, protections, and controls over the components. Stadium and its licensed hosting provider will document the locations that house the critical components, Sports Betting System and maintain a description of the facility and services available, including the following:

- Location description
  - Floor plan
  - Reliability of power and telecommunications
  - Bandwidth availability
  - Compliance of server room to international standards
  - Redundancy of power and telecommunications feeds
  - Offline power capabilities (e.g., UPS and generator power)
  - Refueling requirements of generators and fuel acquisition arrangements
  - Fire suppression system(s)
  - Temperature and humidity control system(s)
  - Procedures for switching to offline power.
- Security description
  - Perimeter boundary fences
  - Use of security guards (employees or contracted)
  - Access controls
  - Alarm systems
  - Video surveillance coverage and storage
  - Monitoring of personnel access to sensitive areas
  - Anti-surveillance measures
  - Tenants
  - Contractors in use for services such as cleaning and maintenance.
- Disaster recovery capabilities, testing, and auditing
- Internal controls

- Visitor access procedures and controls
- Maintenance and audit of access logs
- Alarm procedures for technical and security response
- Due diligence performed on contractors, tenants, and staff
- Emergency access procedures
- Any other relevant procedures.

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.

Communications Security

The Information Systems Officer must ensure that the Sports Betting System is designed to ensure the integrity and confidentiality of all communications and the proper identification of the sender and receiver of all communications. For communications between systems components performed across internet/public or third-party networks, the system will either encrypt the data packets or utilize a secure communications protocol to ensure the integrity and confidentiality of the transmission.

All entry and exit points to the network are identified, managed, controlled, and continuously monitored without interruption. Stadium monitors all Sports Betting Systems in order to prevent, detect, mitigate, and respond to cyberattacks. An intrusion detection, prevention and reporting system is in place on the networks and actively configured to notify system administrators of potential intrusions.

In virtualized or cloud environments, each server instance performs only one function. Stadium maintains security measures to protect against the risks of using mobile computing and communication facilities. Telecommuting is not be permitted except under circumstances where the security of the endpoint can be guaranteed.

If guest networks are offered(such as, networks that provide internet access for players, athletes or participants, or Suppliers), adequate logical segregation is provided 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.

Encryption and Cryptographic Controls

The Information Systems Officer must ensure that encryption and cryptographic controls are implemented, maintained, and supported in WinIn's Sports Betting System as follows:

Component	Encryption and Cryptographic Control
SportsPlay Platform	• All data at rest must be configured with a minimum of AES 256 bit (Advanced Encryption Standard) using symmetric-key encryption with a 256-bit key.
SportsPlay Player Account Management	• All connections, including player sessions, must use HTTPS/TLS1.2 (or higher).
Sports Betting Kiosks	• All connections from the kiosk to the SportsPlay platform, including account management sessions, must use HTTPS/TLS1.2 (or higher).
World Till	• Operating system images installed on desktop and laptop computers must be configured with a minimum of AES 256 bit (Advanced Encryption Standard) using symmetric-key encryption with a 256-bit key. • Encryption employed on desktop and laptop computers must allow for a random cryptographic key to be generated and for the relevant key to be stored in the WinIn's Active Directory (AD).
Local Networking Equipment	• All connections from the kiosk to the SportsPlay platform, including account management sessions, must use HTTPS/TLS1.2 (or higher).
Wide Area Network	• All WAN connections will use TCP/IP and, therefore, must use HTTPS/TLS1.2 (or higher).

a) All PII and betting information passed over networks is protected as per the requirements of high-risk data as established in WinIn's policies and procedures.

b) Stored PII and other sensitive information on portable computer systems, including end user devices (e.g., laptops), removable media (e.g., USB devices), and sensitive information held at rest on Wagering Equipment.

Component	Encryption and Cryptographic Control
Desktops and Laptops	• Operating system images installed on desktop and laptop computers must be configured with a minimum of AES 256 bit (Advanced Encryption

Component	Encryption and Cryptographic Control
	Standard) using symmetric-key encryption with a 256-bit key. • Encryption employed on desktop and laptop computers must allow for a random cryptographic key to be generated and for the relevant key to be stored in WinIn's Active Directory (AD).
Mobile Devices	• All WinIn provided mobile phones must be configured to force the use of a pin code lock which includes a minimum of eight characters. While the use of a PIN alone to secure a mobile phone does not constitute encryption, it does play a vital role in supporting mobile device encryption. • WinIn managed mobile Apps which are authorized for use, and which may process or handle personally identifiable data must use encryption to protect data. • WinIn authorized apps must use secure HTTPS/TLS1.2 (or higher) when communicating over the internet or any other unspecified network connection.
Portable Storage Media	• All portable storage media must use encryption. • Users must set a password for accessing the device. • The password for encrypted, portable devices must be in accordance with WinIn's password policy. • Using the portable device on any other computer after being encrypted will require a password to access it.
Wagering Equipment	• PII is not stored permanently on wagering equipment. Any wagering equipment that connects to the SportsPlay platform must use cryptographic keys.

a) With regards to encryption keys, the following controls must be in place:

   i. Cryptographic keys must be generated, stored, and managed in a secure manner that prevents loss, theft, or compromise.

   ii. Access to cryptographic keys must be restricted to authorized individuals.

   iii. Cryptographic keys must be transmitted by reliable and secure methods to maintain confidentiality and integrity. Separate communication channels should be used for key and data transfer. Under no circumstances should the key and encrypted data be transferred together via the same medium.

b) Integrity measures for the storage of winning wager ticket and voucher data and validation information must be implemented as described earlier.

c) The roles and responsibilities of IT Personnel for key management and the implementation of the cryptography policy are as follows:

    i. The Information Systems Officer is responsible for the implementation of the cryptography policy.

    ii. The IT personnel is responsible for implementation and maintenance of all cryptographic controls, including ensuring they are active at all times.

Firewalls

The Sports Betting System is equipped with a firewall that records the audit information to preserve and secure the information from loss or alteration.

Third-Party Systems

Stadium manages oversight of third parties who provide key support and services. Formal data processing agreements are in place when Stadium shares sensitive information with third-party service providers. The agreement states the rights and obligations of each party concerning the protection of the sensitive information. Each data processing agreement sets out:

- Subject matter and duration of the processing.
- Nature and purpose of the processing.
- Type of data to be processed.
- How the data is stored.
- Detail of the security of the data
- Means used to transfer the data from one organization to another
- Means used to retrieve data about certain individuals;
- Method for ensuring a retention schedule is adhered to
- Means used to delete or dispose of the data
- Categories of data.

Information Security Management System (ISMS)

ISMS Plan

The Information Systems Officer must implement, maintain, regularly review and revise, and comply with a comprehensive Information Security Management System (ISMS) plan to protect the confidentiality, integrity, and availability of personal identifiable information ("PII") of individuals who place a wager with Winin, 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 Winin.

The ISMS plan contains:

- 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.
- A description of how cybersecurity and information security roles and responsibilities of WinIn personnel and relevant third-party service providers Sports Betting System and/or its components.
- A reference to IGT's policies and procedures that support cybersecurity and information security activities within the organization.
- Requirements for planned reviews when changes occur to the Sports Betting System or processes which alter the risk profile of the system.
- Communication of cybersecurity and information security policies to all employees and relevant third parties.
- Protection of sensitive information from unauthorized access.
- The creation of required logs, with controls to prevent unauthorized modification.
- Proper controls and documentation for changes and updates to the Sports Betting System.

The WinIn Security Committee, which is a security forum comprised of senior managers, including the Head of Security or equivalent, has been 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.

ISMS Security Officer

The Information Systems Officer is WinIn's ISMS Officer on an ex-officio basis. The ISMS Security Officer to assure day-to-day compliance and to be responsible for all areas of IT. The ISMS officer must do the following:

- Serves as the primary liaison to executive level management and the Commission for all matters regarding all aspects of cybersecurity and information security.
- Evaluates IT staff and recommends changes needed to ensure protection of the IT infrastructure.
- Oversight of a standard for the proper segregation of IT job duties, including appropriate levels of account privileges.
- Oversight of IT security training
- Aspects of Stadium's investigation and response to IT security related incidents.
- Monitoring employee access and ensuring deactivation of accounts assigned to terminated or suspended employees.
- Review the results of any vulnerability scans and penetration tests, including oversight of the resulting corrective action plans.
- 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 must be developed to address segregation of responsibilities, password administration, implementation of access controls and monitoring intrusions and security violations.

ISMS Audit

The ISMS undergoes an annual audit for review of cybersecurity and information security principles in relation to confidentiality, integrity and availability. Stadium leverages the results of prior audits conducted by accredited vendors, 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. Stadium utilizes a

cloud environment, as allowed by the Commission, to store, transmit and process sensitive information.

WinIn's Sports Betting System must undergo an annual audit against common cybersecurity and information security principles in relation to confidentiality, integrity, and availability, as covered within these Internal Controls. 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.

ISMS Risk Management and Assessment

The ISMS officer maintains the risk management framework for the Sports Betting System. In developing this framework, the ISMS Officer must:

- Utilize quantitative and qualitative analysis to identify and rank all critical components Sports Betting System based upon risk;
- Document the criteria used to determine risk for each critical component of the Sports Betting System; and
- Establish minimum security standards for all critical components Sports Betting System based upon risk.

The risk assessments to identify, quantify, and prioritize risks against criteria for risk acceptance will be performed according to the following methodology:

- Scope Documentation
  - Identify all components of the Sports Betting System.
  - Document the purpose of each component.
  - Document the flow of information in the information systems infrastructure that is within the scope of the risk assessment.
- Risk Analysis
  - Identify potential threats and vulnerabilities associated with the information systems infrastructure that is within the scope of the risk assessment.
  - Describe and analyze the potential risks.
  - Identify currently implemented controls to address those risks.
  - Describe the associated risk level.
- Risk Prioritization
  - Determine the residual risk level.
  - Compare residual risk levels to risk acceptance criteria.

- Prioritize risks by assigning them to established categories.
- Issue controls recommendations.

- Risk Assessment Report

  The ISMS Officer must generate a written report that includes all the elements described herein. The report must be submitted to the WinIn Security Committee.

- Review

  The ISMS Officer must perform reviews of the risk assessment at least annually or pursuant to the following events:

- A major update, upgrade, or migration of the Sports Betting System.
- Significant changes in the configuration of its internal network.
- Implementation of information exchange with any third party.
- A security incident.

The decision of whether any of the aforementioned events warrants a risk assessment is the responsibility of the Wining Security Committee.

ISMS Incident Management Procedures

Stadium maintains procedures that provide for responding to, monitoring, investigating, resolving, documenting, and reporting security incidents associated with the Sports betting system. The incident management consists of:

- Definition of a security incident.
- Process for reporting security incidents through appropriate management channels.
- Address management responsibilities and procedures to ensure a rapid, effective, and orderly response to security incidents, including:
  - Handling of different types of security incident.
  - Analysis and identification of the cause of the incident.
  - Communication with impacted parties
  - Reporting of the incident to the appropriate authority.
  - Forensic evidence collection.
  - Controlled recovery from security incidents.

The ISMS Officer will immediately inform the Commission and executive management, including the IT Director, about all security incidents concerning:

- Unauthorized access or disclosure of sensitive information.
- Unauthorized system modification by a third-party.

- Unauthorized destruction of regulated IT assets or data.
- Any attack that compromises the availability or operation of any critical components of the Sports Betting System.

All security incidents must be responded to within twenty-four (24) hours of detection.

Controls: Maintenance of Sports betting systems

Monitoring of Critical Services and Critical Components

Stadium maintains a list of critical services that are required for the continued operation of sports betting, as well as the availability and resilience requirements of those services.

WinIn's critical services to players that are required for continuous operation of sports betting are as follows:

1. IGT SportsPlay Platform

The IGT SportsPlay platform provides the necessary functionality to capture, process, and pay customer betting action. Therefore, any service interruption of the IGT SportsPlay platform, would cause WinIn's sports betting offering to be unavailable. The IGT SportsPlay platform is provided by IGT in a software-as-a-service (SaaS) model.
The IGT SportsPlay platform allows bets to be placed through several channels. In the case of WinIn's operations, the players access the IGT SportsPlay platform through either a kiosk deployed in the premises of an authorized location or through a mobile application (also called a miosk). Therefore, either the kiosk or the miosk must be available and connected to the IGT SportsPlay platform to allow players to place bets.
The availability and resiliency requirements for the IGT SportsPlay platform are as follows:

- Availability
    - The IGT SportsPlay platform must meet an availability target of 99.99% (52 minutes, 36 seconds of annual downtime).
    - The availability target excludes scheduled maintenance periods established by IGT.
- Resiliency
    - The IGT SportsPlay platform must be able to recover from any adverse event or condition that causes unavailability within 1 hour.

- When recovered, the IGT SportsPlay platform must include all data up to 10s prior to the adverse event or condition.

2. Kiosk

The kiosk allows a player to place bets in the IGT SportsPlay platform. The kiosk provides a user interface that can be operated by the player through the kiosk's touch screen. The kiosk is a physical device deployed at an authorized location's premises and, therefore, must be able to connect to the IGT SportsPlay platform through a Virtual Private Network (VPN) to IGT's infrastructure. This is accomplished through WinIn's network, which connects the kiosks to the Internet via a secure connection.

The software that is deployed in the kiosk is part of the IGT SportsPlay platform. That is, there is no separate software component in the kiosk - it is an element of the IGT SportsPlay platform. WinIn's network must be available for the kiosk to communicate with the IGT SportsPlay platform.

In order for the kiosk to operate, it must be connected to a power source. Therefore, even if the IGT SportsPlay platform is available, if the kiosk is not connected to a power source, or there is a power outage at the location in which it is deployed, players will not be able to place bets.

The availability and resiliency requirements for the kiosk are as follows:

7.1.1.2.1 Availability

a) The kiosks must be physically accessible by players during the business hours of IGT's authorized locations.

b) The IGT SportsPlay platform must meet an availability target of 99.9% (43 minutes, 50 seconds monthly downtime).

c) The availability target excludes times outside the business hours of IGT's authorized locations.

7.1.1.2.2 Resiliency

a) The kiosk must be connected to an uninterruptible power source (UPS) that can allow the kiosk to operate for up to eight (8) hours without an external power source.

b) When recovered, the kiosk must include all data up to 1s prior to the adverse event or condition.

3. Miosk

The miosk allows a player to place bets in the IGT SportsPlay platform. The miosk is an application installed in a player's mobile device powered by Android or AppleOS. The miosk

establishes a secure connection between the player's mobile device and the IGT SportsPlay platform using either a mobile network telephone signal or a Wi-Fi connection.
The miosk is distinct from the IGT SportsPlay platform. Therefore, it is possible for the IGT SportsPlay platform to be available, but the player may not be able to place bets because of issues related to the miosk, the mobile phone, or the mobile telephone network.
The availability and resiliency requirements for the miosk are as follows:

- Availability
    - The miosk is physically accessible by players only if their mobile device is powered and unlocked.
    - The miosk platform must meet an availability target of 99.99% (4 minutes, 27 seconds monthly downtime).
- Resiliency
    - The miosk must be capable of recovering from any failure by restarting automatically.

4. WinIn Network

The WinIn Network connects the kiosks located in the authorized locations to the IGT SportsPlay platform. The first segment of the network connects the kiosk itself to a router in the authorized location's premises. The router then connects to an aggregation point via private fiber optic (dark fiber). From the aggregation point, a public cloud connection is used to reach IGT's infrastructure. The connection established between the kiosk and the IGT SportsPlay platform is configured using a VPN, which establishes a secure, private connection from the kiosk to the IGT SportsPlay platform.
In addition, the WinIn Network allows authorized personnel at the authorized location to register payments of winning tickets issued in the kiosks.
The availability and resiliency requirements for the WinIn Network are as follows:

- Availability
    - The WinIn Network must meet an availability target of 99.99% (52 minutes, 36 seconds of annual downtime).
    - The availability target excludes scheduled maintenance periods established by WorldNet.
- Resiliency
    - The WinIn Network must be able to recover from any adverse event or condition that causes unavailability within 1 hour.

The Sports Betting System failures or unavailability of any of its components will be detected and recorded as follows:

- Power failures at Betting Locations: Power outages will be detected through activation of the UPS in the betting location cabinets.
    - UPS Logs: Logs will be recorded using UPS Software connected to Computer. Software Logs power outage with timestamp and length of outage.
    - UPS Firmware: UPS has firmware that records logs of Outages, timestamped, with length of time power was out.
    - Network Perimeter Firewall: Power Outages can be identified and reported by firewall logs when they fail to detect the endpoints. Timestamp and outage length monitored in logs.
- Network Failures
    - Kiosk is connected via Ethernet Cable (Cat 6) to a network jack on wall which is connected to a Network Switch inside a locked cabinet.
    - Microtik has logging features that record outages can be monitored and e-mail alerts.
    - Switch failure is detected by heartbeat miss and reported via logs and email alerts. If no connection is present the logs will show the errors and timestamps. If there is complete equipment malfunction the peripheral devices will show disconnection logs with timestamps.
    - Aggregation point failure can be monitored by the Firewall and alerts be reported via email and logs are kept in Firmware and Device Memory.

If WinIn 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 Compliance Manager must notify the Commission immediately. Such notification shall include:

- A description of the error.
- Risks created or imposed by the error.
- Efforts being taken by WinIn to prevent any impact to the security and integrity of the Sports Betting System."

Logging

Log information is protected against tampering and unauthorized access. Event logs recording user activities, exceptions, and cyber and information security events are generated on each system component in order to monitor and rectify anomalies, flaws and alerts. All logs are stored and regularly reviewed to be presented as evidence. Transaction logging is enabled on all databases.

Exception Reports

Exception reports are generated for significant events or alternations. Stadium will indicate the system's capability of producing an exception report and to what extent this report provides specified information. Significant events or alternations which are tracked include the following:

- 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).
  This control is implemented through the DCFAILOG – Failed Logins Report available in the IGT SportsPlay platform.
- Program error or authentication mismatch.
  This control is implemented through the FRACTAPP – Exceptions Report: Retail Action Approvals and FREXACTA – Exceptions Report: Action Approval available in the IGT SportsPlay platform.
- 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.
  This control is implemented through the FRACTAPP – Exceptions Report: Retail Action Approvals and FREXACTA – Exceptions Report: Action Approval available in the IGT SportsPlay platform.
- Large wins (single and aggregate over defined time period) in excess of a value specified by the Commission, including wager information.
  This control is implemented through the FREXMKST – Exceptions Report: Market Settlement available in the IGT SportsPlay platform.

- Large wagers (single and aggregate over defined time period) in excess of a value specified by the Commission, including wager information.
  This control is implemented through the FREXMKST – Exceptions Report: Market Settlement available in the IGT SportsPlay platform.
- Large financial transactions (single and aggregate over defined time period) in excess of a value specified by the Commission, including transaction information.
  This control is implemented through the FREXMKST – Exceptions Report: Market Settlement available in the IGT SportsPlay platform.
- System voids, past-post voids, in-progress voids, past-post write, in-progress write, overrides, and corrections.
  This control is implemented through the FREXVDBT – Exceptions Report: Voided Bets, FREXVDBTCS – Exceptions Report: Voided Bets CSV, and FREXVBMOCS – Exceptions Report: Voided Bets - Monthly (CSV) available in the IGT SportsPlay platform.
- 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.
  This information is available through reports in the SportsPlay platform administration console.
- Changes that are made to the download data library, including the addition, changing or deletion of software, where supported.
  This information is available through reports in the SportsPlay platform administration console.
- Changes to operating system, database, network, and application policies and parameters.
  Policies and parameters include, but are not limited to:
    - Audit settings (types of events that are monitored and logged).
    - Password complexity settings (minimum length, maximum age, etc.).
    - System security levels (AS/400, QSecurity).
    - Point structure for player loyalty.

  This control is implemented through the FREXPARM – Exceptions Report: System Parameters available in the IGT SportsPlay platform.
- Changes to date/time on master time server.

This control is implemented through the FREXPARM – Exceptions Report: System Parameters available in the IGT SportsPlay platform.

- 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."
  This control is implemented through the FREXEVDC – Exceptions Report: Event Date Changes, FREXPRCH – Exceptions Report: Price (Odds) Change, FREXSLCH – Exceptions Report: Selection Result Changes, and FREXMKCH – Exceptions Report: Critical Market Changes available in the IGT SportsPlay platform.
- Changes to previously established criteria for an event (not including line changes for active events), such as odds, cut-off times, event data.
  This control is implemented through the FREXEVDC – Exceptions Report: Event Date Changes and FREXPRCH – Exceptions Report: Price (Odds) Change available in the IGT SportsPlay platform.
- Changes to the results of a Sports Event or Special Event.
  This control is implemented through the FREXSLCH – Exceptions Report: Selection Result Changes available in the IGT SportsPlay platform.
- Changes to promotion and/or bonus parameters.
  This control is implemented through the FREXMKCH – Exceptions Report: Critical Market Changes available in the IGT SportsPlay platform.
- Adjustments to a Player Account balance.
  This control is implemented through the FREXUSER – Exceptions Report: DC User Profiles available in the IGT SportsPlay platform.
- Changes made to PII and sensitive information recorded in a Player Account.
  This control is implemented through the FREXUSER – Exceptions Report: DC User Profiles available in the IGT SportsPlay platform.
- Deactivation of a Player Account.
  This control is implemented through the DCULMNR1 – User Listing Report available in the IGT SportsPlay platform.
- Negative Player Account balance (due to adjustments and/or chargebacks)
  This control is implemented through the FREXUSER – Exceptions Report: DC User Profiles available in the IGT SportsPlay platform.

- Irrecoverable loss of sensitive information.
  This information is available through reports in the SportsPlay platform administration console.
- Any other activity requiring user intervention or supervisory approval and occurring outside of the normal scope of system operation.
  This information is available through reports in the SportsPlay platform administration console.
- Other significant or unusual events as deemed applicable by the Commission (the internal controls are to delineate what other events are to be logged).
  The SportsPlay platform provides the flexibility to define custom reports on system parameters, therefore, any Commission requirement can be addressed through custom exception reporting.
  Exception reports Sports betting system for significant events or alternations listed above include the following fields as a minimum:
    - Date and time of the significant event or alteration.
    - Unique transaction identifier.
    - Identification of user(s) who performed and/or authorized the significant event or alteration.
    - Description of the significant event or alteration, including data or parameter altered.
    - Data or parameter value prior to alteration.
    - Data or parameter value after alteration.

  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.

  The Compliance Manager, or his/her designee, must review exception reports on a daily basis for propriety of transactions and unusual occurrences. The reviews are aimed at providing reasonable assurance that:
    - Users are only performing activities which have been explicitly authorized; and
    - Possible threats facing the Sports Betting System are being assessed.

All improper transactions or unusual occurrences noted during the review of exception reports are investigated with the results documented. Evidence of the review is maintained for 18 months following the completion of the review. The evidence includes:

- Date and time of the review;
- Name and title of person performing the review;
- Exception report reviewed;
- Exceptions noted; and
- Follow-up and resolution of exceptions.

The Information Systems Officer must ensure that, in instances where exception events are flagged and notified to the Compliance Manager (or a designee), that the following controls are in place regarding the notification:

- A record of the notification must include the date and time of the notification.
- 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 herein.

The responsibility for reviewing the logs (Compliance Manager) is independent of the system administration and user access administration functions and does not have system access to perform any administrative functions in the systems for which the logs are being reviewed. The Compliance Manager may designate another individual, provided that the employee is independent of the function using the system for which the logs are being reviewed.

The Compliance Manager, or his/her designee must perform the exception report review.

- If the Compliance Manager designates another individual, he/she must be a WinIn employee.

If a notification system is used for exceptions in the SportsPlay platform, the notifications will be directed to the Information Systems Officer, or his/her designee. The designee must be a WinIn employee.

Requirements for System Verification

The Chief Operating Officer must ensure a mechanism is in place 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 and are identical to those approved by the Commission. Provisions are made for the verification mechanism to be run at the following times:

- On restart of the Sports Betting System;
- On the incorporation of changed components to the system following the CMP;
- On a scheduled period of not more than 24 hours as determined by the Commission's Executive Director; and
- At any time at the request of the Commission's Executive Director.

A failure of verification of any component of the system will result in an alert being communicated to the Information Systems Officer and the Commission within twenty-four (24) hours. The same notification must be issued to the Commission's Executive Director.

Control Program Verification Listing ("CPVL")

Stadium maintains a CPVL of the critical control program components along with their corresponding digital signatures to ensure there have been no unauthorized modifications. This control is implemented through the FREXPARM – Exceptions Report: System Parameters available in the IGT SportsPlay platform.

Each item in the CPVL has a unique code, version number, and identification characteristic sufficient to ensure that Internal Audit will be able to inspect some or all components at any given time and determine whether they have deviated from the approved version. A member of the IT function is assigned responsibility for changes to each item in the CPVL.
The attributes available through the FREXPARM – Exceptions Report: System Parameters include:

- *Date/Time* – Date and time of the parameter change.
- *Username* – Username of the operator that made the change.
- *OS User* – Operating System username of operator that made change.
- *Machine* –Domain and computer name of machine used to make the change.
- *Terminal* – Computer name of machine used to make the change.
- *Program* – Application used to make the change.
- Action – Type of action performed (e.g., Insert, Update, Delete).

- *(App Code) Parameter code* – (Application Code) The name/code of the parameter.
- *Change Field* – Indicates field that was changed for the system parameter (e.g., Parameter code, parameter description, parameter value).
- *Old value* – Old value.
- *New value* – New value.

The Information Systems Officer, or his/her designee, must address each item in the Control Program Verification Listing.

System Procedures

The Information Systems Officer will be in charge of developing and maintaining system documentation for all in-use components of the Sports Betting System (versions of application, database, network hardware, and operating system), including descriptions of both hardware and software (including version numbers), operator manuals, etc.

Stadium maintains system documentation for all in-use components of the Sports Betting System, including descriptions of both hardware and software, operator manuals, etc. Stadium takes measures to detect, prevent, mitigate and respond to common active and passive attacks. The Information Systems Officer is responsible for implementing policies and procedures, as well as controls to prevent, detect, contain, and correct security violations in the Sports Betting System; and documenting formal proceedings executed on a periodic basis to analyze and manage risk, sanction non-compliance with policies and procedures, and evaluate information system activity.

Whenever a situation is reported that may relate to or constitute a potential security incident, an initial assessment must be made of the potential security incident.

- If the situation is an actual security incident, the Information Systems Officer must identify and implement measures to mitigate, to the extent practicable, the harmful effects of the security incident.
- After implementing measures to mitigate the incident, the Security Officer must immediately report the incident to the Security Committee, and generate a full written report, including its origin, scope, impact, and measures taken to mitigate the incident, and submit the report to the Security Committee.

Procedures for Maintenance

The Information Systems Officer must initially develop and maintain documentation on the responsibilities of WinIn's IT function for the maintenance of the components of the Sports Betting System. The documentation must include:

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

The Information Systems Officer must ensure that Sports Betting System components are provided with adequate primary power and that controls are in place to supply standby backup power in case of a power outage. The standby backup power supply must be sufficient to operate the Sports Betting System for a minimum of four (4) hours. Sports betting network equipment oversight is maintained to ensure its continued availability and integrity. The logs of all routers, switches, firewalls and other network appliances are reviewed on a scheduled basis for any errors, or performance concerns. Sports betting communications records covering network lag, connection speeds, and communications outages are reviewed on a regular basis and corrective action taken if any errors or performance concerns are detected.

User Access Controls

Access Control Policy

Management periodically reviews the Access Control Policy that are based on business and security requirements for physical and logical access to the Sports Betting System and its components. The Access Control Policy ensures that access to the following is restricted and secured:

- System software and application programs
- Data associated with sports betting
- Communications facilities, systems, and information transmissions

Provisioning of Access Privileges

1. Access Control Policy

   WinIn's Access Control Policy defines mechanisms to ensure that logical and physical access to all applications and Sports Betting System components, its associated data, and the facilities where these components are housed, is allowed only to those persons or software programs that have been duly granted access rights.
   All WinIn supervisors, managers, and executives are responsible for ensuring compliance with this Access Control Policy.

   Only WinIn supervisors, managers, and executives can request access to Sports Betting System components, its associated data, and the facilities where these components are housed. Any such access request must be made in writing. No accesses can be granted without a formal access authorization request. No individual can request access without approval by a designated supervisor, manager, or executive. All access authorization requests must clearly identify the individual for whom access is authorized, as well as whether they are an employee, a contractor, or an external user.

   In addition to the WinIn supervisors, managers, and executives that request access rights on behalf of individuals or software programs, all access requests must be authorized by the Compliance Manager. This access can be revoked or suspended at any time if there is evidence that an individual has misused access credentials to Sports Betting components, its associated data, of the facilities where these components are housed. Any individual whose access is revoked or suspended could be subject to disciplinary measures, corrective action, or other sanctions.

   WinIn supervisors, managers, and executives must ensure that:

   - Only the individuals or software programs that need access to applications and Sports Betting System components are granted such access.
   - Access grants to applications and Sports Betting System components reflect the minimum necessary for an individual or software program to perform its assigned duties.

- Any time an individual's job responsibilities change that, an appropriate access request is generated to modify the individual's current access levels or privileges to maintain adherence to the minimum necessary principle.
- Any access grants are revoked whenever access by individuals or software programs is no longer necessary.

2. Provisioning of Access Privileges

The access privilege authorizations, suspensions, or revocations pursuant to 7.8.1 will be captured in writing in the most recent version of the *Systems Access Request Form* (for logical access) and the F*acilities Access Request Form*, which will be filled out by a WinIn supervisor, manager, or executive.

The *System Access Request Form* must identify the specific Sports Betting System components, or its associated data, for which access is being requested and the access level or role that is being requested for each Sports Betting System component. The *System Access Request Form* must be submitted by the WinIn supervisor, manager, or executive to the Information Security Officer. The Information Security Officer will review the access request and validate that all required information has been provided and that the requested access is appropriate.

- The privileges associated with each access level or roles must be only those duly approved by the Compliance Manager.
- The access levels or roles requested must match those that are allowable for the user's job description, as defined in Section 7.8.4, otherwise the access request must be rejected in its entirety.
- Any exceptions to a) and b) above must be approved by the Information Security Officer, Compliance Manager, and the Chief Executive Officer.

The WinIn Information Security Officer will refer the access request to a User Account Technician, who will configure the requested accesses in the different Sports Betting System components.

- Each individual must have only (1) account in each application or Sports Betting System component. Any access requests for a new account in a particular application or Sports Betting System component must be rejected and returned to the sender.
- In cases where an access request indicates a change to an existing user account, but the account does not exist, the access request must be rejected and returned to the sender.

- If the User Account Technician determines that the access request has the defects identified above, the access request must be rejected in its entirety. That is no access grants or modifications to current access can be implemented as a result of the deficient access request.

After the access to the Sports Betting Components have been configured, the access request must be returned to the Information Security Officer, who will verify that the access request has been correctly processed. If the request is approved, the Information Security Officer must save a copy of the *System Access Request Form* in electronic format. Once verified, the credentials associated with the access request must be remitted by the User Account Technician to the user. The User Account Technician must use an *off-channel* method to convey the credentials to the user.

The user's supervisor must generate a *System Access Request Form* whenever a user's access privileges must be modified whenever the individual's job responsibilities change. The Human Resources Manager must generate a request to revoke all user access privileges associated with individuals whose employment relationship with WinIn is terminated. Access revocations must ensure that a set of previously valid access credentials can no longer be used to access the Sports Betting System components, but that any previous activity associated with those credentials is not deleted. Requests to suspend or revoke a user's access privileges may be originated by the user's supervisor, the Information Systems Manager, or the Compliance Manager.

On a quarterly basis, the Information Security Officer must generate reports from every application and Sports Betting System component listing all active users with their configured roles or access privileges. The reports must be grouped by the user's department as per the most recent WinIn organizational chart.

- The Information Security Officer must distribute each department's list to the supervisor, manager, or executive that heads the department.
- The department head will review the list to identify users that should no longer have access rights or whose access privileges do not comply with the principle of least privilege.
- The department head will remit any exceptions to the Information Security Officer, along with a *System Access Request Form* for each instance where user access needs to be revoked or modified.

The *Facilities Access Request Form* must identify the specific facilities, or areas within facilities where Sports Betting System components are housed, for which access is being requested. The *Facilities Access Request Form* must be submitted by the WinIn supervisor, manager, or executive to the Chief Operating Officer. The Chief Operating Officer will review the access request and validate that all required information has been provided and that the requested access is appropriate. The access request to specific facilities or areas within facilities must match those that are allowable for the user's job description, as defined by the Compliance Manager, otherwise it must be rejected in its entirety.

- The facilities and areas to which access is requested must match those that are allowable for the user's job description, as defined by the Compliance Manager.
- If the facilities access request includes any facility housing applications or Sports Betting Systems components, it must be approved by the Information Security Officer.
- Any exceptions to a) and b) above must be approved by the Information Security Officer, the Compliance Manager, and the Chief Executive Officer.

If the request is approved, the Information Security Officer must save a copy of the *Facilities Access Request Form* in electronic format. If the access request is approved, the Operations Manager will identify the accesses requested for facilities of areas within facilities that are managed by service providers or third parties.

- The Operations Manager will generate a written communication to the designated contact for each service provider to request that access be granted and that credentials, including keys, tokens, or proximity cards, among others, are generated for the appropriate individual.
- The Operations Manager will communicate to the individual the procedures to obtain the access credentials.

If the access request is approved, Operations Manager will communicate with the individual the procedure to obtain the access credentials to WinIn facilities of areas within facilities to which access has been granted. Upon being given access credentials, including keys, tokens, or proximity cards, among others, the individual will sign a *Property Receipt Form* and will sign a *Facilities Access Credentials Allowable Use Form*.

The individual's supervisor must generate a *Facilities Access Request Form* whenever an individual's facilities access privileges must be modified whenever the individual's job responsibilities change.

The Human Resources Manager must generate a request to revoke all facilities access privileges

associated with individuals whose employment relationship with WinIn is terminated. Requests to suspend or revoke a user's facilities access privileges may be originated by the user's supervisor, the Chief Operating Officer, or the Compliance Manager. Prior to termination of employment or other circumstances implying a suspension or revocation of facilities access privileges, the individual must return all facility access credentials to the Operations Manager. The Operations Manager will remit any access credentials to service provider or third-party facilities to the service provider or third party's designated contact.

On a quarterly basis, the Operations Manager must generate a report of outstanding access credentials for all facilities, including service provider and third-party facilities, with the access method, and any access restrictions. The reports must be grouped by the individual's department as per the most recent WinIn organizational chart.

- The Operations Manager will distribute each department's list to the supervisor, manager, or executive that heads the department.
- The department head will review the list to identify individuals that should no longer have access rights or whose access privileges do not comply with the principle of least privilege.
- The department head will remit any exceptions to the Operations Manager, along with a *Facilities Access Request Form* for each instance where access needs to be revoked or modified.

Logical Access Control

The Information Security Officer must ensure that all components of the Sports Betting System is logically secured against unauthorized access by authentication credentials that include at least an identifier and an associated password. Any authentication credentials stored on the system are either encrypted or hashed to the cryptographic algorithms established in ISO/IEC 19790:2012 (Information technology — Security techniques — Security requirements for cryptographic modules) or that otherwise meet current industry accepted standards.

Any fallback method for resetting authentication credentials must be at least as strong as primary method and include multi-factor authentication. In cases where an authentication attempt for any identifier fails three (3) consecutive times, the following actions must be taken immediately:

- The account associated with the identifier must be suspended.
- A notification must be issued to the Sports Betting System Administrator and the Information Security Officer.
- The account must only be activated if the user's supervisor or manager submits a request in writing to the Information Security Officer.
- The mechanism to unlock the account must include multi-factor authentication.

User Access Functions

The range of access functions available to each employee is defined by the process owner, IT and Security.

Where passwords are used as an authentication credential, security parameters for passwords, if configurable, must meet the following minimum requirements, which are enforced automatically by the Sports Betting System:

- Passwords must be changed at least once every 90 days. If a user has not changed their password for 90 or more days, the Sports Betting System must force the user to change the password on the next successful login.
- Passwords must be at least 8 characters in length and contain a combination of at least two of the following: upper case letters, lower case letters, numeric and/or special characters.
- Passwords may not be re-used for a period of 18 months; or passwords may not be re-used within the last ten password changes.
- User accounts are automatically locked out after 3 failed login attempts as described herein.

The internal controls 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.

Where user sessions are tracked for authorization, the user session authorization information will be created randomly, in memory, and will be removed after the user's session has ended. Access to administer the network, operating system, applications, and database security and system parameters is limited to IT personnel.

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

For the purposes of this section, administrative access means access that would allow a user to:

- Add, modify, or delete user accounts and associated user provisioning for the database, operating system, and network layers.
- Modify operating system, database, and application security and policy parameters.
- Add, change, or delete system exception logging information.
- Add, change, or delete permissions to data files and folders.

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

- All administrative groups and groups with elevated privileges to ensure membership is appropriate;
- 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);
- Administrative accounts to ensure that passwords have been changed at least once every 90 days; and
- The user list to determine whether IT personnel utilize normal user accounts for regular use and administrator accounts for administrative functions.

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. At least annually, the Sports Betting System is reviewed by personnel independent of the individual who establishes or edits 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 is tested 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).

Removal of Access Privileges

The access rights of employees to the Sports Betting System and/or its components are removed upon termination of employment, contract or agreement, or change. Under no circumstances should the Information Security Officer be unaware of a planned employee termination. The Information Security Officer and the Sports Betting System Administrator 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) by the Human Resources Manager.

In cases of planned voluntary or involuntary terminations of employment, the notification must include the effective date of the termination. Hostile terminations require immediate notification to the Information Security Officer and the Sports Betting System Administrator, who must disable/remove access rights to the systems within the hour of being notified and which should happen before the employee is notified of such hostile termination.

Any time termination involves a person with administrative access, the selected replacement must be ready to assume their duties immediately. The replacement should

be involved in searching for and dismantling any malicious plans that may have been left in place or set into motion by the predecessor.

Generic Accounts

Generic accounts at the application level are prohibited unless user access is restricted to inquiry only functions. The use of generic accounts is limited, and where used the reasons for their use will be formally documented by the Information Security Officer. Generic accounts at the operating system level, if used, are configured such that the user is:

- The user is automatically brought to the application login screen immediately upon logging into the operating system, and the user is logged out of the operating system automatically upon exiting the application; or
- 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 from interactive access to the operating system through the proper security configurations.

The Information Security Officer must document the justification for issuing any operating system-level generic account credentials.

All generic accounts must be secured as follows:

- Each generic account must have a designated owner who is responsible for the management of access to the account. This designation must be included in the Information Security Officer's justification.
- The generic account owner must maintain documentation related to the account, including a list of individuals who have current access to the account and when the individual started using the account.
- The Sports Betting System Administrator must change the account password whenever individuals accessing the account are terminated for any reason or are transferred to a role that does not require access.
- The generic account owner must make all documentation related to the generic account available upon request for an audit or a security assessment as often as quarterly or as defined by the Information Security Committee.

- Network generic account access to workstations will occur only in protected areas where public access is supervised and/or restricted and the account may not be used on workstations in any other area.
- Requests for all generic accounts must be approved by the Information Security Officer.
- The Information Security Officer will review all generic account activity on a quarterly basis for appropriateness of access and ongoing need.

Service Accounts

Service accounts will be used only when absolutely necessary. Service accounts, if used, are utilized in a manner to prevent unauthorized and inappropriate usage to gain access to an application and the underlying databases and operating system. Service account login and password information is restricted to a limited number of authorized employees.

The Information Security Officer must document the justification for using any service account. The Information Security Officer must document every instance in which service account credentials are shared with an authorized employee, including the employee's name and the date in which the credentials were shared. The Information Security Officer must document the methods implemented to prevent unauthorized and inappropriate usage of these service accounts (available upon request by authorized internal and external auditors and by Commission personnel).

All service accounts must meet the following requirements:

- Service accounts are configured such that the account cannot be used to directly login to the console of a server or workstation.
- The Sports Betting System Administrator must change service account passwords are changed at least once every 90 days, and immediately upon termination of any individual with whom service account credentials have been shared, including, but not limited to, system administrators.

Default Accounts

User accounts created by default 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. Any other default accounts that are not administrator, service, or guest accounts are disabled unless they are necessary for proper operation of the system.

The Information Security Officer must document every instance in which default account credentials are shared with an authorized employee, including the employee's name and the date in which the credentials were shared. The Information Security Officer must document the methods implemented to prevent unauthorized and inappropriate usage of these default accounts (available upon request by authorized internal and external auditors and by Commission personnel).

If these accounts remain enabled, the Information Security Officer must document any such exceptions and the Sports Betting System Administrator must ensure the passwords are changed at least once every 90 days, and immediately upon termination any individual with whom default account credentials have been shared.

Test Accounts

Stadium establishes test accounts that are used by the Commission or Stadium employees to test each of the various components and operations of the Sports Betting System.

The Compliance Manager must initiate all requests for the creation, modification, or inactivation of test accounts. The Compliance Manager must document every instance in which test account credentials are shared with an authorized user, including the user's name and the date in which the credentials were shared. In the case of test accounts intended for external users (e.g., Puerto Rico Gaming Commission users), the Compliance Manager must ensure they are only active during the period in which the test accounts will be used.

Test accounts are subject to the following controls:

- The Information Security Officer and the Chief Operating Officer must approve all test accounts associated with the Sports Betting System and its critical

components, as well as approving all testing activity and assignment of test account for use.

- The Chief Operating Officer must define and implement procedures for the Issuance of funds used for testing, including who is authorized to issue the funds and the maximum amount of funds that may be issued.
- The Compliance Manager must maintain a record for all test accounts, including when they are active and to whom they are issued.
- The Compliance Manager must define and implement procedures for the audit of testing activity to ensure accountability of funds used for testing and proper adjustments to reports and records.

List of Accounts

System administrators maintain a current list of all enabled human or system accounts(List of Accounts), whether intended for use by individuals or processes. The List of Accounts must include the following elements, at a minimum:

- Name of system (i.e., the application, operating system, or database);
- User account login name;
- Description of the account's purpose; and
- A record (or reference to a record) of the authorization for the account to remain enabled

The current list is reviewed by IT management in addition to the system administrator at least once every six months. The Sports Betting System Administrator must ensure that the List of Accounts contains all enabled accounts, whether intended for use by individuals or processes, and including generic accounts, service accounts, default accounts, and test accounts.

The Information Systems Manager must ensure that:

- All accounts intended for use by processes are still necessary.
- All accounts are configured following the *least privilege* principle.
- All generic accounts, service accounts, and default accounts are not enabled for remote access.

- All generic accounts, service accounts, and default accounts are properly documented with regards to their justification and to whom the credentials have been shared.

The Information Security Officer must ensure that for enabled accounts for use by individuals, other than those reviewed by the Information Systems Manager:

- All accounts are still necessary.
- All accounts are configured following the *least privilege* principle.
- All accounts are properly documented with regards to their authorization.

Each of the individuals tasked with reviewing the List of Accounts must issue a report identifying any unnecessary access accounts, improper privileges, deficient documentation, or any other exception to the internal controls.

- Any findings of unnecessary accounts must be referred to the Sports Betting System Administrator so that the accounts can be disabled.
- Any findings of improper privileges must be referred to the Sports Betting System Administrator so that the account privileges can be configured to reflect the findings from the report.

The Compliance Manager must review the reports generated as a result of the review of the List of Accounts, including evidence of disabled accounts and modification of account privileges pursuant to the applicable provisions herein. The purpose of the review is to evaluate whether the method used is a properly designed control process and is effectively operating to secure the generic, service, and default accounts from unauthorized usage.

User Access List

The Sports Betting System will generate a monthly User Access Listing, which must include, at a minimum, all access changes, and changes in authentication credentials. This includes the creation, modification, and inactivation of user accounts, the associated account access privileges, and the date and time in which the actions were taken on the user accounts. The changes in authentication credentials must distinguish between

instances where the password was changed voluntarily versus those in which the Sports Betting System forced the change in credentials.

The User Access Listings (In pdf format) must be sent automatically to a read-only folder or other logical location where the reports cannot be modified. The User Access Listings must also be generated in a comma-delimited file stored in the same read-only folder or logical location as the report listed above.

The list is reviewed quarterly by personnel independent of the authorization and user provisioning processes. The review consists of examining a random sample of at least 10% (with a maximum of 25) of the users included in the list for:

- Assigned system functions used as authorized (i.e., system functions are appropriate for user's job position).
- Assigned functions provide an adequate segregation of duties.
- Terminated employees' user accounts have been changed to inactive (disabled) status within the time period determined by management. . 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 reason for not performing a verification of time period is document.
- 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.
- 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.

The Internal Auditor must maintain adequate evidence to support the review process for the last four quarterly periods. The evidence includes:

- Date and time of review.
- Individual(s) performing the review.
- Selected user accounts reviewed.

- Documentation of the results of the review, including exceptions, follow-up and resolutions.

User Access Logging

The Sports Betting System will log all actions performed on the Sports Betting System by human or system accounts. The logs must be monitored, regularly reviewed, and acted upon as appropriate by the Information Security Officer.

Control 44: Remote Access to the Sports Betting System

Remote access allows a user access to Stadium's Sports Betting System in IGT's private cloud through the use of a Virtual Private Network (VPN) connection. All remote access to the Sports Betting System must be strictly controlled as described in this section. Remote access to any component of the system is configured to prevent the transfer of Personally Identifiable Information (PII) outside of the United States and territories, unless authorized by the Commission.

Remote access to the system components (production servers, operating system, network infrastructure, application, database, and other components) is limited to authorize IT personnel employed by Stadium, except in the following cases:

- Provider to any component of the system is allowed for purposes of support or updates and is enabled only when approved by authorized IT personnel employed by Stadium. If the remote access to a database is performed by an unlicensed Provider, the remote access is continuously monitored by IT employed by Stadium.
    - IGT personnel may be allowed access to the production servers, operating system, application, database, and other components, except the network.
    - WorldNet personnel may be allowed access only to the network.
    - If the remote access is performed by Provider personnel whose access request has not been processed as described in these Internal Controls, the remote access must be continuously monitored by WinIn IT Personnel.

- Stadium will provide the Commission remote access to wagering transactions and related data as deemed necessary by and in a manner approved by the Commission.
- Remote access may be allowed for non-IT Personnel. However, non-IT Personnel is precluded from directly accessing any databases or operating systems of any of the Sports Betting System and other production environment servers and multi-factor authentication is required for all access requests.

Remote access to Player Accounts by authorized employees of Stadium from outside of the United States and the Commonwealth of Puerto Rico is not permitted at any time. All WinIn employees are within Puerto Rico's geographic limits and, therefore, no special procedures are necessary for remote access.

Provider accounts are restricted through 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. Stadium employs security methods in addition to passwords, including, but not limited to, multi-factor authentication, to verify the identity of the Provider prior to authorizing any remote access. User accounts used by Providers remain disabled on all operating systems, databases, network devices, and applications until needed. Subsequent to an authorized use by a Provider, the account is returned to a disabled state.

- Any instance of remote access to Sports Betting System components are automatically recorded by a device or software in a remote access activity log. At least quarterly, the remote access activity will be reviewed by Internal Audit. The review consists of examining all remote access sessions and non-Provider personnel (IT employee, management personnel, or other authorized employee). For each of the instances of remote access, the Internal Auditor must determine whether: Each remote access session by a Provider has been appropriately documented;
- The remote access was requested by an authorized individual or process;
- The individual or process was properly authorized as established in the internal controls;

- The remote access sessions originated from authorized hardware (e.g., servers, devices).;
- The remote access sessions originated from authorized locations;
- The remote access accounts that are no longer necessary have been disabled as established in the internal controls.; and
- Passwords associated with remote access have been changed within the last 90 days.

The Internal Auditor must maintain adequate evidence of the review of remote access activity logs for the previous four quarters. The evidence is to include at a minimum:

- Date and time of review;
- Name and title of person(s) performing the review;
- Remote access activity log reviewed; and
- Documentation of the results of the review, including any exceptions, follow-up and resolution of exceptions.

Software Downloads

The Information Security Officer must ensure that all downloads use secure methodologies that deliver the download data without alteration or modification. Downloads conducted during operational periods are performed in a manner that will not affect sports betting. Downloads do not affect the integrity of locally stored data. Stadium, through its Information Security Officer, records the following information for each download:

- The times and dates of the initiation and completion of the download;
- The system components to which software was downloaded;
- The version(s) of download package and any software downloaded;
- The outcome of any software verification following the download (success or failure); and
- The name and identification number, or other unique identifier, of any individual(s) conducting or scheduling a download.

Backup and Recovery Procedures

The Information Security Officer must ensure that daily backup and recovery procedures are in place and follow a process documented in the internal controls. 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 Information Systems Manager is the employee responsible for reviewing the backup logs.

Backup data files and data recovery components are managed with the same level of security and access controls as the Sports Betting System for which they are designed to support. The Information Systems Manager must initially develop and maintain e documentation indicating the procedures implemented for the backup processes and for restoring data and application files.

At least on a quarterly basis the IT personnel tests the recovery procedures. A record is maintained indicating the date a test of the recovery procedures was performed and the results of the test. The recovery procedures must include, but are not limited to, the following:

- Data backup restoration;
- Program restoration; and
- Redundant or backup hardware restoration.

Contingency Plan

The Information Security Officer must lead and coordinate the initial development, subsequent maintenance, annual updating, and testing of 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. The plan, which shall be updated annually, considers disasters caused by weather, flood, fire, environmental accidents, malicious destruction, acts of terrorism or war, and contingencies such as strikes, epidemics, pandemics, etc. If a virtualized or cloud environments will be used to support the

Contingency Plan, the Compliance Manager will ensure that a request for approval is submitted to the Commission.

The Information Security Officer must develop and implement a process for testing the Contingency Plan at lease annually. The Information Security Officer must issue a report detailing the results of the test that is sent to the Commission within one month after the completion of the test. All recommendations for improvements are documented and implemented by the Information Security Officer.
The roles and responsibilities for maintaining the Contingency Plan are as follows:

- Information Security Officer
  - Leading the Contingency Plan review and update process.
  - Identifying any changes in the backup and recovery strategy and associated procedures.
  - Identifying any facilities used to support Contingency Plan recovery activities.
  - Requesting and securing support from WinIn operations and administration areas, as necessary, to perform the review and update process, including the determination of recovery priorities.
- Information Systems Manager
  - Generating a list of all applications, systems, and IT services that must be recovered as part of the Contingency Plan.
  - Providing information related to systems suppliers and service providers that must support Contingency Plan activation and associated recovery activities.

The Information Security Officer must furthermore plan, perform, and evaluate contingency exercises in regular intervals to prepare WinIn for crisis situations, covering the elements included in the Contingency Plan.

General Operating Procedures

Protection of Unpaid Funds

Stadium secures funds related to unpaid winning tickets and vouchers before and after the end of the redemption period.

The protection process includes the following measures:

- Stadium's Sports Betting System keeps track of wagers and unpaid winning tickets and vouchers. Additionally, its access controls are strict and include the following: (i) firewalls to ensure no outsiders have access to the system; and (ii) key controls and segregation of duties to ensure no single employee is able to manipulate the system.
- By keeping strict accounting standards and tracking unpaid winnings on real time, the Company ensures that its bank account contain reserves to cover expected payouts.
- The calculation for the amount of unpaid winning tickets and vouchers is made more efficiently and effectively by having all employees perform the following tasks:
    - Confirm the validity of winning tickets/vouchers redeemed
    - Verify that the player is paid the appropriate amount;
    - 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;
    - Follow these Internal Controls regarding ticket redemption to ensure that each redeemed ticket/voucher cannot be redeemed again;
- The Company's Sports Betting System also has features to protect unpaid winning tickets and vouchers:
    - Winning tickets and vouchers cannot be redeemed if the Sports Betting System is not working or should the Sports Wagering Facility be closed;
    - Winning wagers are honored for 180 days from the event's outcome;
    - Winning tickets and vouchers must be cashed out within 180 days from the event's outcome;
    - The system maintains information to audit the final transfers upon wager settlement and voucher redemption for 5 years;
    - Redeemed tickets and vouchers are automatically marked as such within the Sports Betting System to ensure that the same ticket or voucher cannot be redeemed at another authorized location;

    - The payout of lost or defaced winning tickets or vouchers must be authorized in writing by at least 2 employees, including the retail supervisor; and,
    - Any late or last-minute payouts must be authorized in writing by at least 2 employees, including the retail supervisor and the Retail and Operations Manager.
- The Sports Betting System protects itself by blocking any unauthorized access attempts. The human component is essential to protect the Sports Betting System and employees have the responsibility of reporting any unauthorized access attempts in writing to their direct supervisor as well as the Company's Chief Operating Officer and activating the escalation process for any incident or suspicious activity, which must be informed in writing to the Company's Chief Financial Officer and Chief Operating Officer.
- Finally, the Sports Betting System maintains audit trails that are able to identify unusual patterns of late payouts. Such audit trails are inspected on a weekly basis by the Compliance Manager and the Chief Financial Officer to determine any transactions to be reviewed and any further action to be taken to ensure unpaid funds are protected in compliance with the MICS.

Operator to Player Communications

E-mail and text message (SMS) communications to players for advertising purposes will be managed by WinIn's Marketing Department. For outgoing marketing SMS and e-mail communications to players, WinIn will use an API from a third-party provider. Upon registration and confirmation of their legal age to gamble, WinIn will seek players' specific consent to enroll in our promotional program to receive marketing material and exclusive offers via e-mail and/or SMS .

Regarding communications to players via SMS, WinIn will comply with the 1991 Telephone Consumer Protection Act, as amended (47 U.S.C. §227), and observe the Cellular Telephone Industries Association's (CTIA) Messaging Principles and Best Practices and the third-party provider's applicable policies. Similarly, WinIn's marketing e-mails will be compliant with the CAN-SPAM Act of 2003 as amended (15 U.S.C. §7701-7713), and its related regulations codified in 46 C.F.R. Part 136.

WinIn will periodically offer players a straightforward mechanism to opt-out and/or unsubscribe from our promotional program to prevent any future marketing messages from us. Accordingly, WinIn will endeavor to act promptly on the opt-out request to ensure that after opting out, those players will not receive further marketing emails or SMS.

Moreover, WinIn's outgoing promotional SMS and e-mail content and practices will further comply with WinIn's Privacy Policy, our Terms and Conditions, and the company's advertising policies (that models AGA's Responsible Marketing Code for Sports Betting) set forth in our Responsible Play Plan, attached hereto as an exhibit. Marketing communications to players will be retained for a minimum period of ninety (90) days.

Any other communication to players, regarding disputes or customer service and support will be managed accordingly by our Customer Service Department. Communications pertaining to customer support or services will be kept for a minimum period of ninety (90) days and communications regarding customer disputes will be retained for a minimum period of five (5) years.

Advertising

The Operator's Responsible Play Plan, attached hereto as an exhibit, meets the Regulations' requirements for "Advertising" and covers the items listed within the "Responsible Marketing Code for Sports Betting" posted on the American Gaming Association (AGA) website at www.americangaming.org.

Responsible Play

Stadium maintains a Responsible Play Plan, attached hereto as an exhibit, that has been approved by the Commission. The Plan includes:

- Goals and procedures
- Identification of the individual(s) responsible for the implementation and maintenance of the plan

- A training plan for employees who may interact with players, including annual or periodic refresher training. Training will enable the employee to respond to circumstances in which gambling activity may indicate signs that are consistent with gambling addiction.
- Duties and responsibilities of employees designated to implement or participate in the plan.
- An estimation of the cost of development, implementation and administration of the Responsible Play Plan.

Prevent Extension of Credit or Promotion

Stadium prohibits any personnel from extending credit to an individual, group of individuals, or entity that places wagers with or seeks to place wagers with Stadium. Credit providers such as small amount credit contracts (payday lending) are not advertised or marketed to players. A player will not be referred to a credit provider to finance their sports betting activities. Sensitive information related to a player will not be provided to any credit provider. Stadium will 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 Stadium.

Authorized Sports Betting

Wagers on Sports Events and Special Events

The framework in which Stadium offers sports betting and the House Rules are defined, maintained, and published, including all authorized events and wager types for each Sports Event or Special Event. 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. This includes wagers related to:

- Any occurrence related to the conduct of a Sports Event and Special Event.
- Individual athlete or participant performances in ancillary events.

- Conduct or outcome of professional league. Wagers related to each round of the draft will cease upon the commencement of that round.
- Any award granted or recognized by the Sports Governing Body or equivalent. Wagers related to each award will 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 will be demonstrated to the Commission that the voting for such awards is collected and tallied:
    - 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.
    - In a manner that maintains the confidentiality of the outcome until the award is announced.
- Excludes wagers which are related to:
    - Injuries;
    - Officiating calls; and
    - Other unsportsmanlike conduct.

New Events

Stadium may petition the Commission for approval of a new event upon which wagers may be placed or accepted. If Stadium would like to offer a new category of event or wager type, it will 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 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.
- Stadium shall submit the following information within the Category of Sports Betting Request Form:
    - Stadium's name as the petitioner;
    - 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;

- 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;
- A full description of any technology that would be utilized to offer the new event or wager type;
- Information or documentation that demonstrates that the granting of the request for approval would be consistent with the public policy of the Commonwealth;
- Request for a test of the new event or wager type;
- 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
- Any other pertinent information or material requested by the Commission.

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 it deems appropriate.

The Executive Director shall approve, deny, or request further information within fourteen (14) days of submission. If the Executive Director takes no action within that period, Stadium may offer the requested sports betting unless the Executive Director issues a subsequent disapproval.

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, for new events approved for other operators, Stadium 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.

Except as otherwise provided herein, 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.

Wagering Periods

A Wager can only be placed on a given Sports Event or Special Event if the wagering period is open.

Placement of Wagers

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

The placement of bets through the assistance of a teller, requires the teller to log in to Stadium's betting platform, the World Till. The teller must launch the World Till and log in with his or her own employee user identification and password. Tellers are required to log in and log out before and after every shift. At the end of the shift Tellers are required to print out a reconciliation report. World Tills are enabled with the functionality to generate reconciliation reports.

Company managers or supervisors may assume the role of sports betting writers or tellers to perform all necessary related duties, including the writing and paying of tickets. In such case, such person's supervisor or an employee at least one level above in hierarchy pursuant to the organizational chart will handle the revision of the reconciliation report.

Sports betting management will have administrative terminal access for the sports betting system to perform all administrative functions.

Pre-Play Wagering

Pre-play wagers will be placed prior to the start time of the Sports Event or Special Event. At the discretion of Stadium, 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 at the time the pre-play wager is placed.

In-Play Wagering

Stadium monitors the integrity of in-play wagering, the results handling and player protection. Areas for consideration include, but are not limited to, time delays, sources of results, reversal of results, and delays in live pictures.

Placing a Bet

When betting, players will be able to select the sports event or special event in which they want to place a bet on. Bets may be done according to the following types:

a. Straight or Fixed Odds Bets: Bet where the payout is to be fixed at the time the bet is placed. If the predictions are correct, the odds are first multiplied by each other and then by the amount of the bet.
b. Pari-Mutual Bets: Bet where individual bets are gathered into a pool. The winnings are calculated by sharing the pool among all winning bet, subtracting the takeout or fees established by the Company.
c. Crossed or Exchange Bers: Bet where the Company acts as the intermediary and guarantor of the amounts wagered between third parties, subtracting the established company takeout or fees.

The Company will accept players to place in cash, cash equivalent, vouchers, promotional funds, or player account funds. Bets can be placed in a Kiosk, a Ticket Writer Station or other window locations located in an authorized retail location, or through the use our Mobile App or Site.

A wagering account must be created by a player before any bet will be accepted from a player betting account.

No Company employee will accept a bet from a person who the Company knows or reasonably should know is placing the bet for the benefit of another for compensation or is placing the bet in violation of state or federal law.

Ticket Writer Stations

Whenever a ticket writer station is opened/closed or turned over to a new teller, the teller must sign on/off. Each user is allocated a unique login and password that must be kept secure and private. Upon each login/logoff, an entry is recorded in the system that cross-references the user login to the database session with the teller's identity, the date and time, station number and whether the station was opened or closed.

Bet acceptance

Upon accepting a bet at an authorized retail location, a bet ticket is produced and issued to the player containing the following information:

a. The date and time the wager was placed;
b. The date and time the event is expected to occur (if known);
c. Player selections involved in the wager:
    i. Wager selection (e.g., each athlete or participant);
    ii. Event and line postings (e.g., money line bet, point spreads,
    iii. over/under amounts, etc.);
    iv. Any special condition(s) applying to the wager;
d. Total amount wagered, including any promotional/bonus credits
e. Total amount of potential prize, including any promotional/bonus credits
f. Unique Kiosk ID, Ticket Writer Station ID, or user ID of employee which accepted the wager;
g. Unique wager ID
h. A barcode or similar symbol or marking, corresponding to the unique wager ID
i. the name and address of the authorized retail location; and
j. where and how the ticket can be redeemed.

Note: If a bet is placed using the mobile application, then a betting ticket does not need to be created. All betting conducted through the mobile application will be electronically recorded and retained for a period of 60 days.

A restricted computer system record is created concurrently with the generation of the original betting ticket. The restricted record is not accessible to employees except for inquiry only functions.

Wager Cancellations and Voids

Wagers will not be modified except to be voided or cancelled as provided for in the published cancellation policy. A cancellation grace period may be offered to allow players to request a cancellation of wagers placed. Player initiated cancellations may be

authorized in accordance with the cancellation policy. Any cancelled wager will be refunded upon request by a player.

The Sports Betting System is configured to void and cancel wagers. A wager will not be declared void or cancelled in the system without the approval of a supervisory employee. Stadium 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 player used funds that were incorrectly credited to their Player Account to purchase the wager.
- The outcome of the event is known or a material advantage has occurred, regardless of its outcome.
- 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.
- Stadium cannot satisfactorily determine the event results as provided in the House Rules.
- Stadium determines a player placed the wager illegally or otherwise violated the House Rules.

The Company further reserves the right to void or cancel any bet if it 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, the following circumstances:

- The wager was placed with incorrect statistical data;
- Human error in the placement of the wager;
- The wager ticket does not correctly reflect the wager; or
- Equipment failure rendering a wager ticket unreadable.

Stadium will cancel a wager under the following circumstances:

- Where a Sports Event or Special Event which the subject of the wager is cancelled, postponed or rescheduled to a different date prior to completion of the event.

- 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.
- Stadium establishes a timeframe in which an event may be rescheduled or postponed without canceling the wager. This timeframe is related to specific events, subject to the approval of the Commission, and documented.
- 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.
- When ordered by the Commission.

Stadium will prevent the voiding or cancellation of wagers after the outcome of an event is known without the prior approval of the Commission. Stadium will request the Commission to order the cancellation of all wagers of a specific type, kind, or subject. A request to cancel will be in writing, and contain the following:

- Type of wager Stadium is requesting to cancel;
- Facts relevant to the request; and
- Explanation why cancelling the wagers is in the best interests of the Commonwealth or ensures the integrity of the sports betting industry.

No wager subject to the request to cancel will be redeemed until the Commission issues an order granting or denying the request to cancel. If the Commission grants the request to cancel, Stadium will make commercially reasonable efforts to notify players of the cancellation along with a reason for cancellation. Stadium will cancel a wager made by a Prohibited Player and refund the amount wagered. Stadium will cancel a wager at the time they become aware or should have been aware that the player is a Prohibited Player:

Betting ticket's cancellations or voids require approval from a supervisor. If an employee voids a betting ticket, the following procedure must be followed:

- The computer brands the voided ticket with the word "void" and date/time stamps the ticket with the computer system updated to reflect the voided transaction. If the system fails to properly scan or brand the voided ticket, the ticket shall be manually scanned or the ticket number manually entered to update

the system to reflect the voided ticket. The word "void" must be stamped or written on the ticket.

- Tickets voided prior to the start of an event are recorded on the computer-generated exception report, which lists the time the ticket was written and the time of the void.
- For tickets voided during system downtime, the date and time the ticket was voided is stamped on the original, and the ticket void recorded in the system once the operation is restored.
- Voided tickets must be signed by a teller or teller and a supervisor at the time of the void.
- If the original ticket is unavailable (e.g., printer malfunction), a supervisor will reprint the ticket using the reprint option available in the system. The void will then be processed under the above procedure.
- If the voiding machine/stamp is not available for any reason, including a malfunction, the employee may handwrite the word "VOID" on the printed ticket in an indelible ink in a prominent fashion. The employee must also ensure that the wager is also voided in the database.

Timing for Bet Acceptance or Voids

A sporting event bet will not be accepted after the start of the event unless "in progress" or a similar notation is indicated on the original and each copy of the betting ticket, and the system creates and maintains a record that documents the supervisor's approval. Start times can be overridden by a supervisor's access code only from an administrative terminal. Such overrides are recorded on an exception report for each occurrence.

Note: The second half of a football game, for example, is considered a separate event when set up in the system as an independent event for accepting wagers; accordingly, supervisor approval does not need to be recorded as long as the wager is accepted before the start of the second half.

Race wagers are not accepted after post time, the computer automatically locks the game/race out.

Wagering cutoff times are established and entered into the system. The system will not allow a ticket to be voided after an event is locked out unless a lockout is overridden by a supervisor. Such voided tickets are shown on the computer Exception Report as past post voided tickets. The system is incapable of accepting a cutoff/starting time (including changes to cutoff/starting times) that is earlier than the current time of day.

Tickets will not be written or voided after the outcome of an event is known.

Procedures for Mobile Account Wagering

All mobile account wagering administrative activities will be conducted within WinIn's offices in Puerto Rico.

The system will provide permit players to review and confirm all wagering information prior to acceptance of the wager. The system will create a record of the confirmation. This record of the confirmation of the wager will be deemed to be the actual transaction of the record, regardless of what wager was recorded by the system.

The system is configured to prohibit wagers from being changed after player has reviewed and confirmed the wagering information, and the specific wagering communication transaction has been completed.

The system is configured to prohibit the acceptance of wagers after post time.

The system is configured to disallow or prohibit an account wager, or a series of account wagers, in an amount in excess of the available balance of the wagering account.

The system prohibits acceptance of any off-property wagers.

Winning account wagers will be posted as a credit to the player's wagering account as soon as all the results of the wagered events are declared official and posted to the system.

The system maintains complete records of every deposit, withdrawal, wager, winning payoff, and any other debit or credit for each account

Placing a Bet Through the Mobile App

A bet is placed through the mobile app by the following method:

a. Log into the application with your account username and password,
b. Select the sport, team/game wanted
c. determine the dollar value of the bet;
d. Select or press the "Place Bet" button to submit the wager. Note: Prior to selecting the "Place Bet" button there is an option for player to edit their wager prior to submission.

Note: The system will only accept bets from players with a username and assigned personal identification number reasonably designed to prevent the acceptance of wagers from a person other than the player for whom the wagering account was established.

Winning Wager Ticket and Voucher Payment

Payment of Winnings

The Sports Betting System is configured to pay winning wagers and is restricted to prevent unauthorized access and fraudulent payouts by one person. Stadium documents the:

- Identification of the employee authorized (by position) to make a payout.
- Predetermined payout authorization levels (by position).
- Procedures ensuring separate control of the cage accountability functions.

A Company teller will pay a winning ticket through a terminal located at an authorized retail location. An additional terminal will be located at the Main cage. This terminal will be used by cage personnel only for bet payouts.

The Company will withhold payment of a winning ticket if player refuses to provide a valid identification.

The Company will state the redemption period on each betting ticket, 180 days, and on notices conspicuously placed about the licensed premises.

Prior to payment of winning wagers, results of events are entered into the computer through an administrative terminal.
Prior to making payment on a ticket or crediting the winnings to the player's account:

- The teller scans the player's ticket and verifies the ticket in the computer system to authorize payment; or
- For wagering account bets, when the event results are posted in the computer system, the sports system automatically authorizes payment of winning bets and updates the player's account.

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. If an employee manually enters or scans the wager ticket/voucher number into the 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, and the amount of payment and date.

Checkout Standards

The Sports Betting System indicates the amount of net cash that should be always in each teller station. This information is accessible to supervisors.

At the end of a shift, or whenever there is a change of teller during a shift, the teller will close the till, and a shift summary report is generated by the supervisor and the following procedures are performed:

- The outgoing and incoming teller count the cash drawer down and record on a check-in/check-out slip by denomination the funds in the drawer, any variances in the count are noted on the check-in/check-out slip.
- The outgoing and incoming teller sign the check-in/out slip attesting to the accuracy of the count.

Withholding Delinquent Child Support from Winnings

In compliance with Administrative Order OACJAD-22-08 issued by the Commission on January 31, 2023, once the Commission has established the platform to submit quarterly information to the Commission and the Administration for Child Support Enforcement ("ASUME"), Stadium shall prepare such reports including 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; and

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.

Redemption during System Failure

Stadium maintains manual procedures that have been approved by the Commission that will be used during system failure. In case of Sports Betting System failure, winning wager tickets/vouchers may be paid. If tickets are paid during a system failure a log is maintained that includes the following:

- date and time of the system failure;
- reason for failure; and
- date and time the system is restored.

For all payouts, including payouts for contest/tournament winners that are made during a system failure, thus without system authorization, the following procedure will be followed:

- After the manual grading of the winning wager ticket/voucher, the date and time will 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;

- Before completing the payout, the Retail and Operations 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
- Once the system is operative, an employee will immediately enter all manually paid wager tickets/vouchers to verify the accuracy of the amount paid for the wager tickets/vouchers and the manual grading of the wager tickets.

The teller will keep the ticket for all payouts made in situations where results are not entered into the computer or in case of computer failure

Note: Any manually paid wager tickets that had been previously purged from the system does not need to be entered into the system.

The system is designed to prevent payment of a ticket that has been previously paid by the system, voided by the system, a losing ticket, or a ticket not issued by the system.

Taxation Reporting

In compliance with Administrative Order OACJAD-22-08 issued by the Commission on January 31, 2023, Stadium's Sport Betting System identifies all wins that are subject to taxation, that is, net winnings in excess of five hundred dollars ($500) within a calendar year, which are subject to taxation reporting as follows:

a. For Puerto Rico residents, Stadium's accounting function shall complete and file Puerto Rico Treasury Form 480.6A "Informative Return – Other Income Not Subject to Withholding".

b. For non-Puerto Rico residents, Stadium's accounting function shall complete and file Puerto Rico Treasury Form 48.6C "Informative Return – Payments to Nonresidents or for Services from Sources Outside of Puerto Rico".

i. Payments to foreigners that do not live in Puerto Rico or the United States shall be subject to a 29% withholding.

ii. Payments to United States citizens that do not live in Puerto Rico shall be subject to a 20% withholding. However, United States citizens that do not live in Puerto Rico may request an exemption from such withholding by completing Puerto Rico Treasury Form AS 2732 "Withholding Tax Exemption Certificate in the Case of Nonresident Individuals – Citizens of the United States".

In compliance with the Puerto Rico Internal Revenue Code, these informative returns shall be submitted on an annual basis to the Puerto Rico Treasury Department and the players through electronic means or regular mail, as established by the Treasury Secretary pursuant to regulations, administrative determinations, circular letter or informative bulletins.

Lost Wager Tickets and Vouchers

The Retail and Operations Manager or a supervisor may approve the redemption of a lost or stolen wager ticket or voucher. The following documentation must be obtained when redeeming lost wager tickets:

- The date and time of the redemption;
- The employee responsible for redeeming the wager ticket or voucher;
- The supervisor authorizing the redemption;
- The name of the player redeeming the wager;
- Unique wager ticket or voucher identifier; and
- Location of the redemption.

Payout Process for Mail-In Winning Wager Tickets and Vouchers

All mail-in ticket payments are received and logged by the Executive Assistant or someone authorized from Finance. The log will contain the date the mail-in ticket or wager was received, name of player and the wager/voucher ticket number(s). The mail-in tickets and log will be forwarded to accounting for payment and audit purposes.

Questionable tickets will be forwarded directly to the Retail and Operations Manager or related personnel, where it will be examined for validity.

Only Accounting supervisors are authorized to approve mail-in payments.

Accounting enters the ticket number into the system. The system validates the ticket and documents the ticket as paid. Accounting writes/stamps paid on the ticket with the date and amount paid.

A check request is signed by an accounting supervisor and is forwarded to the accounts payable office for payment. Accounts payable will compare the redeemed winning ticket, the mail in log, the system report for paid winning tickets and check request for any discrepancies. Accounting is informed of any discrepancies, which are investigated and corrected prior to payment.

Layoff Wagers

WinIn may, in its discretion, accept a Layoff Wager placed by another Licensed Operator (referred to as, the "Other Operator"). The Other Operator placing a Layoff Wager must disclose its identity to WinIn's employee taking the wager.

The amounts of bets placed by the other Operator and the amounts received by WinIn as payments on such bets will not affect the computation of WinIn's Adjusted Gross Revenue.

Before WinIn accepts a bet from another Operator, the following shall take place:

a. The authorized employee of the other Operator must personally appear at one of WinIn's Authorized Locations to register and open a Player Account;
b. WinIn's employee will request and record the following information:
    i. The name of the other Operator's authorized employee, permanent business address (other than a post office box number), and business telephone number;
    ii. The documents to verify the Operator seeking to place the Layoff Wager is a Licensed Operator (i.e., copy of the Operator's License), the authorized employee's employee identification and a letter from the Operator authorizing such employee to open the Player Account with WinIn on the Operator's behalf.
    iii. The amount of the other Operator's Initial Player Account or front money deposit;
    iv. The authorized employee's account number with the other Operator; and
    v. The date the authorized employee of the other Operator opened the account with WinIn;
c. The authorized employee of the other Operator must sign, in the presence of a WinIn's supervising employee, statements attesting the following:
    i. Confirms the accuracy of the information recorded;
    ii. Has received a copy, or has had a copy made available to them, of the WinIn's rules and procedures for wagering communications;
    iii. Has been informed and understands that, upon opening a Player Account pursuant to these Internal Controls, they are prohibited by law from placing wagering communications from outside the Commonwealth of Puerto Rico and that WinIn is prohibited, by law, from accepting them;
    iv. Consents to the monitoring and recording by the Commission and WinIn of any wagering communication; and
    v. WinIn's employee, who verifies the authorized employee of the other Operator's information and who obtains and records the information on behalf of WinIn, and the supervising employee described herein 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.

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

Bonus or Promotional Payouts, Drawings and Giveaway Programs

Stadium may offer bonus or promotional payouts. The rules and conditions for participating in bonus or promotional payouts are available to a registered player on the website where the bonus or promotion is being conducted and are prominently displayed or available for player review at the Authorized Location.

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

- 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;
- Restricted player funds 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;
- Winnings from restricted player funds are able to be withdrawn without being subject to any further wagering requirements;
- Bonus or promotional payouts are not transferable between Player Accounts;
- Stadium will provide a method for a player to cancel their participation in a bonus or promotion that utilizes restricted bonus or promotional payouts;
- Upon request for cancellation, Stadium will 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;
- If the player elects to proceed with cancellation, unrestricted player funds remaining in a Player account will be recounted in accordance with the conditions of the promotion or bonus;
- Closure of the Player account will render a promotion or bonus void; and
- Once a player has met the conditions of the promotion or bonus, Stadium will not limit winnings earned while participating in the offer (i.e., the restricted player funds will become unrestricted player funds).

Bonus or promotional payouts and verification consist of:

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

- Documentation completed in respect of bonus or promotional payouts include the following information:
    - The date and time;
    - 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;
    - The type of bonus or promotion;
    - The reason for payout (e.g., bonus or promotion name);
    - Player's name and confirmation that identity was verified (drawings only); and
    - 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.
- The documentation 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.

Player Loyalty Programs

Player loyalty programs may be established by the Company as a way for players to accumulate points, based on the volume of wagering reflected in their account. These points may be subsequently redeemed by for wagering credits, cash, merchandise, etc.

The rules and policies for the player loyalty program including the awarding, redeeming, and expiration of points are available to registered players 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.

Player loyalty information is stored in a database that permits inquiry and reporting activities in addition to routine, scheduled reporting. The addition/deletion of player loyalty points, other than through an automated process, related to actual wagering is recorded and authorized/performed by appropriate supervisory personnel. This does not

apply to the deletion of points related to dormant and closed accounts through an automated process. Points may be automatically deleted in dormant and closed accounts.

Stadium will remove excluded persons from player loyalty programs.

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.

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

Changes to the player loyalty parameters, such as point structures and employee access, is performed by supervisory personnel independent of the sports betting function. Alternatively, changes to player loyalty account parameters may be performed by the Retail and Operations 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.

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

Complimentary Services or Items

Stadium maintains procedures for the authorization, issuance, recording and monitoring of complimentary services or items, including cash and non-cash gifts, and documents the following:

- Delegation of authority to employees to approve the issuance of complimentary services or items, including levels of authorization;
- Limits and conditions on the approval and issuance of complimentary services or items;
- Changes to conditions or limits on the approval and issuance of complimentary services or items;
- Documenting the authorization, issuance, and redemption of complimentary services or items, including cash and non-cash gifts; and

- Provisions for audit purposes.

On a monthly basis, the accounting, IT, or audit personnel that cannot grant or receive complimentary privileges will prepare reports that include the following information for all complimentary items and services equal to or exceeding $100:

- The name of player who received the complimentary service or item;
- The name(s) of issuer(s) of the complimentary service or item;
- Actual cash value of the complimentary service or item;
- The type of complimentary service or item; and
- The date the complimentary service or item was issued.

Internal Audit or Accounting will review the reports at least monthly. Complimentary services and items records are summarized and reviewed for proper authorization and compliance with established authorization thresholds. A detailed reporting of complimentary services or items transactions that meet an established threshold approved by the Commission are prepared monthly and reviewed by management.

Contests and Tournaments

Stadium may organize and conduct a contest/tournament, which permits a player to either purchase or be awarded the opportunity to engage in competitive wagering against other players. Contest/tournament rules are available to a registered player and are prominently displayed or available for player review at the Authorized Location. A player will register prior to participating in a contest/tournament and the player will provide the following information:

- Name;
- Date of birth; and
- E-mail address.

Note: Only players with a confirmed wagering account will be allowed to register to participate in any contest/tournament conducted by the Company. Moreover, the Company may request additional documentation to verify that player is 18 years of age or older prior to registration or before issuance of awards.

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

- Player's name;
- The date of entry/payout;
- Amount of entry fee/payout and/or nature and dollar value of any non-cash payout;
- 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; and
- The name of the contest/tournament.

Stadium's accounting function will identify, record, and document all funds collected and distributed for contests and tournaments.

The contest/tournament entry fees and payouts are summarized and posted to the accounting records on a monthly basis. One entry, in total, for contest/tournament entry fees and payouts will be posted on a monthly basis to the general ledger.

On a weekly basis, 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.

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

Sports Betting Risks and Controls

Company management team, along with assistance from their service providers, continually monitors odds, betting patterns, line movement, and irregularities on a daily basis.

Events, Odds and Result Management

Stadium maintains a process for validating accuracy and preventing fraudulent activities. The process is based on the respect of integrity, player protection, and ensuring transparency and involve several levels of authority. Logs and other audit trails exist to prevent possible misuse of authority. Stadium ensures authorized payout levels are not exceeded.

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

Stadium will resolve errors for purposes of resettlement including, operator errors or if 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.

Monitoring Activities and Reporting Fraud and Suspicious Conduct

Stadium monitors all changes to odds/payouts and prices and/or blocking throughout a Sports Event or Special Event the events and player transactions for the detection of irregularities, winners with gains over $3,000, and deposits over a certain size. Stadium specifies thresholds of payment and methods of collection.

Stadium 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.

Stadium monitors for unusual and suspicious activity and reports such activity in accordance to Stadium's procedures that have been approved by the Commission. If, in the course of doing business, anything is encountered that is not consistent with normal betting patterns that may compromise the integrity of a game or outcome of an event, the surveillance department will submit a Suspicious Activity Report describing the suspicious activity to the CEO, COO or his designee. Stadium shall share copies of information with other Operators as necessary, and will share all reports of unusual and suspicious activity to the Commission immediately but no later than 12 hours after the suspicious activity has been identified. Management will also run reports that document the date, time, odds or line movement of the game(s) in question, along with the amounts of the wagers and descriptions of individuals making the wagers. If the Company receives notice of any suspicious activity occurring at another property, the surveillance department will respond to the Commission within 12 hours to confirm or deny any similar betting trends and activity.

Stadium will Monitor and report unusual and suspicious activities such as, but not limited to the following:

- Attempts to violate or evade any local or federal law or regulations pertaining to sports betting;
- Violations or attempted violations of local or federal Anti-Money Laundering (AML) laws;
- Unusual or suspicious behavior or patterns of Wagers by Player as determined by Stadium; Unusual geographical concentration betting;
- Wagers that have been placed online or through a mobile device using different accounts but having the same IP address;
- Access of accounts with the same IP address from foreign jurisdictions;
- Unusual and abnormal proportion of bets against the favorite or the underdog; and
- Unusual volumes of betting relative to the norm.

Stadium will 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. If Stadium has knowledge or reasonable suspicion of suspicious

activity, it may determine suspend wagering on related events but will only cancel or rescind related wagers after receiving the Commission's approval. Stadium will 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.

Global Risk Management

Stadium does not currently have the intent to utilize Global Risk Management. In such case, Stadium shall submit information about its chosen provider, including a copy of the written agreement for those services. Stadium understands that 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.

As established by the MICS, 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:

- Setting, modifying, or providing risk management advice as it relates to odds, point spreads, and lines;
- 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;
- Determining when the wagers placed by Players on a particular Sports Event or Special Event should be rejected;
- Determining when it would be desirable to place layoff wagers with another licensed Operator in the Commonwealth; or
- Using their special expertise to manage the risks associated with Sports Betting in the Commonwealth.

If Stadium determines to engage in global risk management, it may provide direction, management, consultation, and/or instruction to another Operator located in a permissible jurisdiction concerning:

- The management of risks associated with sports betting involving a Sports Event or Special Event for which a wager may be accepted;
- 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;
- Whether or not to accept or reject wagers, to pool wagers, or to layoff wagers;
- The use, transmittal, and accumulation of information and data for the purpose of providing global risk management; and
- 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.

Stadium recognizes that if it intends to provide global risk management, it shall:

- 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;
- 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;
- 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
- Provide such other information as the Commission may require concerning global risk management.

Additionally, at least 30 days prior to providing global risk management to another licensed Operator in the Commonwealth, Stadium would submit to the Commission the written agreement for the global risk management provided to the other licensed

Operator in the Commonwealth. Stadium understands that the Commission may object in writing to such agreements in the Commission's sole and absolute discretion. If the Commission objects to an agreement, Stadium shall not provide global risk management to the other licensed Operator in the Commonwealth until Stadium has resubmitted the agreement to the Commission, and the Commission has indicated in writing that the Commission does not object to the resubmitted agreement.

Location Service Providers

Stadium, or a third-party Location Service Provider (LSP) used by Stadium, provides location-based services and the border control technology for the identification of the geographic location of players. Stadium, or the LSP, undergoes a specific annual audit to review the following:

- Confirmation of a player's location and the location of their access device that is shared with Stadium or LSP contractors, sub-contractors, affiliates and other third-parties.
- Stadium 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.
- The border control technology used for location detection:
    - Utilizes closed-source databases (IP, proxy, VPN, etc.) that are updated daily and periodically tested for accuracy and reliability.
    - Undergoes quarterly to maintain 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.
    - The Commission is provided evidence quarterly that the border control technology is updated to the latest solution.

Authorized Location

Hours of Operation

Stadium's Authorized Locations shall only operate according to the hours approved by the Commission. Stadium will submit a proposed schedule to the Commission 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.

During authorized hours, Stadium 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 as well as the payments of the winnings.

If any of Stadium's Authorized Location has to shut down due to unforeseen circumstances and the closure is unscheduled, Stadium shall immediately inform the Commission.

Betting Counters and Windows

Each of Stadium's Authorized Locations shall include betting counters and windows that shall be designed and constructed to provide the maximum security for the materials stored and the activities performed at such locations, including a secure location for the purpose of storing funds issued by a cage to be used in the operation of sports betting. Additionally, each shall include one or more betting windows, each of which shall contain a cashier's drawer and Ticket Writer Station through which sports betting financial transactions are conducted and a physical barrier designed to prevent direct access to the materials stored and activities performed at such betting counter. If required by the Commission, an Authorized Location shall include manually triggered silent alarm systems, which shall be connected directly to the surveillance monitoring room and have an alarm for each emergency exit door that is not a mantrap.

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

- Physical barriers are installed to prevent unauthorized individuals from direct access to the area containing the Ticket Writer Station and safe.

- Physical security will be available to prevent unauthorized individuals from direct access to the area containing the Ticket Writer Station and safe.
- Surveillance cameras provide coverage of individuals placing wager and individuals accepting wager.

When temporary betting counters are not in use:

- All financial instruments are removed from the cash register/safe and Ticket Writer Stations are locked to prevent unauthorized access;
- Surveillance camera requirements noted above will remain in place irrespective of the betting counters being moved to different locations; and
- Surveillance cameras shall continue to monitor the area and will be supplemented by physical security personnel, as needed.

Main Cage

Computer Applications

Stadium's computer systems run the World Till, which are the hardware and software components deployed at authorized locations to handle player service requests. Stadium's computer shall not operate any other applications, except those that are installed by default as part of its operating system. However, for any computer applications that Stadium expects to utilize in the future, it will ensure to have procedures that provide at least the level of control described by the MICS in this section, as approved by the Commission.

Account Controls for a Main Cage

An Authorized Location has a main cage that has been approved for the operation by the Commission. Stadium only conducts 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. Each betting window and counter has a dedicated cash register/safe for the storage of financial instruments. The movement or physical transfer of financial instruments are restricted to the count staff and/or security. Records and documentation of deposits and withdraws from cash register/safe are maintained and include the names of individuals performing the function including dollar amounts of financial instruments, date and time of transactions.

A cage supervisor or equivalent shall be available at all times during which sports betting is taking place. Ticket Writers have a valid, unexpired, occupational license issued by the Commission. Stadium will perform the following:

- 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;
- Validate winning wager tickets and vouchers;
- Process payment or transfer of winnings;
- Maintain a reserve bankroll sufficient to pay all winning wagers;
- Compute reserve cash bankroll requirement daily;
- Submit computation to the Commission:
    - At least 30 days prior to the commencement of sports betting operations;
    - Within 24 hours of Stadium determining that the reserves are not sufficient to cover the calculated requirement; and
    - Annually in which a license is issued; and
- The Ticket Writer Station is secured through password, biometrics or other similar means. Generic passwords for the Sports Betting System are prohibited for cashiers.

Each ticket writer redeems wager tickets and vouchers from the ticket writer's assigned window. After verifying the winning wager ticket/voucher in the Sports Betting System, the cashier will sign 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/voucher in the cashier's cash drawer.

Each ticket writer is assigned a unique date/time stamp used solely at the ticket writer's assigned window. Payouts of $3,000 or more, or those exceeding any tax reporting threshold, requires the supervisor to enter an approval code and to sign the wager ticket. Deposits, withdrawals, or payouts of $10,000 or more also requires the supervisor to enter an approval code and to sign the wager ticket/voucher.

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 Stadium's end-of-shift report. Any discrepancies noted and investigations performed are documented and maintained.

When a supervisor signs onto a common terminal with their individual password, they take responsibility for the sports betting payouts. Operational procedures detail the process to reprint tickets/vouchers that fail to print at either a Ticket Writer Station or Kiosk. The supervisor authorizes all reprints. Stadium provides the Commission with the start and end time of each cage shift. The times do not change without prior Commission approval.

Employee Segregation of Duties

Company personnel with the authority to create/cancel events, adjust times on events, open/adjust betting lines, enter event results, suspend events, and approve voids, do not have the ability or authority to write or cash tickets.

Stadium maintains segregated duties of the main cage, and the general conduct of the main cage transactions. Ticket writers are responsible for:

- Individual inventory of cash;
- Receipt and payout of cash, negotiable instruments, vouchers, and other records from and to players
- Preparation of wager ticket records; and
- Other functions designated by Stadium which are not incompatible with the functions of a ticket writer.

Main bank cashiers or others approved by the Commission are responsible for:

- Receipt of cash, negotiable instruments, vouchers, and other records from ticket writers in exchange for cash or documentation;
- Receipt of unsecured cash and unsecured vouchers;
- Receipt of cash and documentation from the count room;

- Preparation of the overall main cage reconciliation;
- Preparation of bank deposits;
- Compliance with reserve bank roll requirements;
- Receipt of original and redemption copies of counter checks;
- Receipt from ticket writers of documentation supporting counter check substitution, consolidation, or redemption; and
- Other functions designated by Stadium which are not incompatible with the functions of a main bank cashier.

Employees who perform the supervisory function of approving wager ticket voids do not write wager tickets unless:

- The only supervisory function allowed is approval of wager ticket voids prior to post time.
- A supervisor, acting as a writer, may not authorize a void for a wager ticket which he wrote.
- All wager tickets written by a supervisor which are subsequently voided and all not-in-computer voids are 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.
- The log is provided to a function independent of the sports betting function on a daily basis for a 100% audit of void wager tickets for the proper signatures (includes occupational license number), a void designation, date and time of the void(for not-in-computer voids), any indications of past-post voiding, and other appropriate regulation compliance. Any discrepancies noted and investigations performed will be documented in writing and maintained.
- A function independent of the sports betting function will perform a 100% audit of the exception report for any inappropriate use of the supervisory password. Any discrepancies noted and investigations performed is documented in writing and maintained.

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 permitted to switch for certain shifts or days to having cashier functions.

Stadium shall prohibit any employee who is serving alcoholic beverages to customers from taking sports wagers during the same work shift.

Finally, to ensure segregation of duties, employees authorized to destroy redeemed winning wager tickets and vouchers shall be formally defined. Stadium's platform keeps track and control of redeemed winning wager ticket and void tickets. Provided that players can keep the printed tickets, Stadium will not keep such printed tickets as part of its official records. However, as a supplementary safety measure, void tickets may be destroyed by Stadium if requested by a player. Such destruction shall be handled by the teller's supervisor, unless such supervisor served such client. In such case, the supervisor must have the teller perform the physical destruction.

Cage Access

Stadium restricts physical access to the cage to only cage employees, designated staff, and other authorized persons. Stadium allows limited transportation of extraneous items such as personal belongings, toolboxes, beverage containers, etc., into and out of the cage.

Cage Accountability

Stadium ensures that all transactions that flow through the main cage within the Authorized Location are accounted for. This includes:

- All transactions that flow through the cage are summarized on a cage accountability form on a per shift basis and are supported by documentation.
- Increases and decreases to the total cage inventory is verified, supported by documentation, and recorded. Documentation includes 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).

- At the end of a shift, the ticket writers assigned to the outgoing shift conducts the following:
    - Face value of each cage inventory item counted and the total of the opening and closing cage inventories; and
    - Reconcile the total closing inventory with the total opening inventory.
- At the conclusion of each operational day, copies of the cage accountability forms and all supporting documentation are provided to the Accounting function.
- Signature requirements are established for outgoing and incoming ticket writers.

The cage inventories are counted independently by the incoming and outgoing ticket writers. They make individual counts for accuracy and individual accountability. The counts are attested to by signature and recorded at the end of each shift during which the activity took place. All variances of more than $500.00 are documented and investigated. Unverified transfers of financial instruments are prohibited. Stadium maintains financial instruments) in an amount sufficient to satisfy obligations to the players as they are incurred.

Ticket Writer Station Reconciliation of Assets and Documents

A Ticket Writer begins a shift with a set amount of financial instruments ("Sports Betting Inventory"). No funds will be added to or removed from the sports betting inventory during the shift except in:

- Collecting wagers;
- To make change for a player buying a wager ticket;
- Payment of winning or properly cancelled and refunded wager tickets;
- Payment for vouchers ; and
- Exchanges with the main cage, a satellite cage, or betting counter supported by proper documentation that is sufficient for accounting reconciliation purposes.

Whenever a ticket writer exchanges funds with the Main Bank, they prepare an Even Exchange form. The form includes the following information:

- Date of preparation;
- Window location;

- Separate areas designating which items are being sent to/received from the Main Bank;
- Type of items exchanged;
- Total of the items being exchanged;
- Signature of the ticket writer preparing the form; and
- Signature of the main bank cashier completing the exchange.

Each ticket writer and main bank cashier prepares a "Sports Betting Count Sheet" on each shift that includes recording the following information:

- Amount of inventory in the betting window or bank;
- Reconciliation of the total closing inventory with the total opening inventory.;
- Signature and employee occupational license number of the incoming and outgoing ticket writer or main bank cashier:
    - Date, time and shift of preparation;
    - Total amount of each denomination of currency in the drawer;
    - Total of any exchanges;
    - Total amount in the drawer;
    - Value of the sold, voided, and cashed wager tickets or a printout from the system to the count sheet;
    - Total amount of financial instruments in the sports betting inventory issued to the Ticket Writer;
    - Betting window number to which the Ticket Writer is assigned; and
    - 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.

A Ticket Writer assigned to a betting window will count and verify the Sports Betting inventory in the count room and will reconcile the count to the "Sports Betting Count Sheet". The sports betting inventory is placed in a ticket writer's drawer and transported directly to the Ticket Writer station by the Ticket Writer. At the end of the operational day, the main cage will forward a copy of each ticket writer's "Sports Betting Count

Sheet" and related documentation to the accounting function for agreement of opening and closing inventories and comparison of forms or documents.

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 will record overages or shortages on a Ticket Writer Variance log. If the count does not agree, the ticket writer and the shift supervisor will 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, the discrepancy will be reported in writing to the Retail and Operations Manager, or supervisor in charge, and documentation will be provided to the accounting function. Any discrepancy in excess of $500.00 is reported to the surveillance function and the Commission within two hours of the supervisor's shift ending, utilizing the Commission's incident report form.

The shift supervisor will 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 equal the wagering count sheet total plus the wagering inventory, the shift supervisor will sign the Sports Betting Count Sheet attesting to its accuracy. Stadium will determine the daily win amount by comparing the Win Summary Reports from the system to the reconciliation of the sports betting drawers. Stadium reports sports betting revenue as the higher amount unless otherwise authorized by the Commission.

Kiosks

Kiosks Identification

Every Kiosk has the following identification characteristics:

- Certificate of license issued by the Commission; and
- A permanent printed label stamped and visibly affixed to the upper left of the kiosk cabinet display. It is assigned and set by the Commission to each approved Kiosk. The following are characteristics of the label:
    - Unique identification number;
    - Number of the inspection certificate; and

- Assigned to a specific kiosk and cannot be removed or transferred for use in another Kiosk.

Kiosks Restrictions

Kiosks are configured so that they are unable to:

a. Process deposits and withdrawals to player wagering accounts of $10,000 or more;

b. Issue or redeem a voucher with a value of $1,500 or more;

c. Redeem a wager ticket with a value of $1,500 or more; and

d. Redeem a wager ticket or voucher with a value which exceeds any Tax Reporting Threshold.

Access to Kiosks

Stadium ensures that only authorized, registered employees of Stadium, registered employees at an Authorized Location, and a Commission licensed supplier, may access the secure area of a Kiosk. Stadium requires that all doors of the Kiosks be secured at all times and the recording of relevant entries in a log each time a Kiosk is accessed.

Kiosk Cash Storage Box

Each cash storage box used with a kiosk has an asset number permanently imprinted, affixed or impressed on its outside, which can be clearly seen and readable by the CCTV System. This number corresponds 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.

Collecting Currency Cassettes and Cash Storage Boxes from Kiosks

Stadium ensures that currency cassettes and cash storage boxes are securely removed from Kiosks on a daily basis, unless otherwise agreed to by the Commission. Surveillance personnel are notified prior to the cash storage boxes or currency cassettes being accessed in a Kiosk. The drop is monitored and recorded by surveillance. Stadium submits

the drop schedule to the Commission and includes the time the drop is scheduled to commence, and the number and locations of Kiosks

At least two employees are involved in the collection of currency cassettes and/or cash storage boxes from Kiosks, and at least one employee is independent of Kiosk accountability. Currency cassettes and cash storage boxes are secured in a manner that restricts access to only authorized employees. Redeemed vouchers and winning wager tickets (if applicable) collected from the Kiosk are secured and delivered to the Cage or Accounting for reconciliation.

A Security function member and a Main Cage function member 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. A function member independent of Kiosk responsibility will place the empty cash storage boxes needed for the drop into a secured cart and prepare a drop form, which includes the following:

- The date;
- The identification number of the secured cart;
- The number of empty cash storage boxes placed into the secured cart; and
- The signature of the Main Cage function employee documenting that the number of cash storage boxes equals the number of Kiosks in use.

In the presence of a Security function member, a Main Cage function employee will complete the drop at each Kiosk by:

- Unlocking the cabinet housing the cash storage boxes;
- 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;
- Locking the cabinets housing the cash storage boxes; and
- Transporting the secured cart to a count room or other location approved by the Commission for the count of the drop.

Kiosk Count and Documentation

Kiosks are counted independently by at least two employees, documented, and reconciled for each increase or decrease to the Kiosk inventory. Access to stored full cash storage boxes and currency cassettes is restricted to authorized employees and, in an emergency, authorized persons for the resolution of a problem. The Kiosk count is performed in a secure area, such as the cage or count room.

Cash storage boxes and currency cassettes are 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. The contents of the cash storage boxes are counted by two or more accounting personnel with no incompatible function, and they must perform the following:

- Document the contents, by item and amount, for each cash storage box on a balance receipt;
- Prepare drop total reports that summarizes total currency, wager tickets, and vouchers counted;
- 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 are documented on this form);
- Transfer the currency to a main bank cashier with a copy of the drop totals report;
- Transport the wager tickets and vouchers to a secured location approved by the Commission for storage until permitted to destroy; and
- Provide the balance receipts, the drop totals report and drop form to the Accounting function.

The contents of each removed currency cassette and reject bin is counted by two or more Accounting personnel with no incompatible function, who:

- Documents the count of each currency cassette and reject bin on a balance receipt, by Kiosk.

- Prepares a currency cassette replenishment totals report that summarizes the total currency counted.
- Transfers the currency to a main bank cashier with a copy of the currency cassette replenishment totals report.
- Transports balance receipts and currency cassette replenishment totals report to the Accounting function.

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

Kiosk Replenishment

Currency cassettes are secured with a lock or tamper resistant seal and, if not placed inside a Kiosk, are stored in a secured area of the cage or count room. On a daily basis or at a greater frequency as needed, Stadium replenishes the currency cassettes in the Kiosks. A cashier with no incompatible functions prepares the currency cassettes to replenish the Kiosks, which are documented on a two-part cassette fill form. The cashier retains one copy of the form and the duplicate is used to document the completion of the transaction. The form includes the following information:

- Designation of the Kiosk to which the fill is to be performed;
- For each denomination, the number of bills and total value;
- Total value of all currency cassettes;
- Date and time prepared; and
- Signature of the cashier.

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

Stadium's employees are trained to operate its kiosks in accordance with all manufacturer manuals. By following all kiosk manuals and implementing such procedures,

Stadium ensures that currency cassettes contain the correct denominations and have been properly installed.

Kiosk Reconciliation of Assets and Documents

When 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.

The Accounting function reconciles the Kiosks on a daily basis, and whenever employees remove winning wager tickets, vouchers or cash from a Kiosk. Any variance of $500.00 or more is 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 indicates the cause of the variance and contains any documentation required to support the stated explanation. Winning wager tickets and vouchers are delivered to the Accounting function.

Count Room Access and Count Team

Stadium limits physical access to the count room to count team employees, designated staff, and other authorized persons. Applicable controls include the following:

- Count team employees do not exit or enter the count room during the count except for emergencies;
- Surveillance personnel is notified whenever count room employees exit or enter the count room during the count; and
- Extraneous items such as personal belongings, toolboxes, beverage containers, etc., should not be brought into the count room.

Stadium ensures the security of the count and the count room to prevent unauthorized access, misappropriation of funds, forgery, theft, or fraud. Applicable controls include the following:

- All counts are be performed by at least two employees.

- At no time during the count will there be fewer than two count team employees in the count room until the drop proceeds have been accepted into cage accountability.
- Functions performed by count team employees are rotated on a routine basis.
- Count team employees are 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.

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) is maintained and available to the Commission upon request.

Wagering Equipment

Certification

Before deployment of any product, software, or equipment, and thereafter, annually, the Company will procure, as applicable, its audit, testing and certification from an independent testing laboratory in accordance with the standards set forth in GLI-33, the Commission's MICS, the Law, and the Regulations.

Time & Date

The time and date reflected in the system, Atlantic Standard Time, is kept accurate through a connection to an independent automated update process using Network Time Protocol (NTP).

The time/date stamp equipment is directly and permanently wired to the electrical system. Only authorized employees will have access to the power control mechanisms used in connection with the stamping equipment. Any testing log produced will be made available to the Commission upon request.

Only Company authorized personnel, independent of the ticket writing functions, test the time/date stamp equipment for accuracy to the nearest minute at least once each day. These tests, and any adjustments necessary due to discrepancies, are documented on a

log, which includes the station number, date, time of test, time on machine, name or signature of employee performing test and any other relevant information.[1]

All date and time stamping of voided tickets is performed on the same ticket writing station as the one used for the issuing of the original ticket.

Where applicable, keys (original and duplicates) to the time/date stamping equipment are issued only to security or authorized personnel for adjustment or testing purposes only.

ADA Compliance

Stadium's Authorized Locations, as holders of use permits issued by the Permits Management Office of the Commonwealth of Puerto Rico, comply with the requirements of title III of the Americans with Disabilities Act of 1990, 42 U.S.C. §§ 12181-12189 ("ADA"), and its implementing regulations.

Wagering equipment shall be installed to ensure accessibility to the greatest number of potential players. Stadium personnel shall be available at all times to assist any players with disabilities in the placement of their bets.

Shipping and Receiving Equipment

Software and hardware components shall be shipped by their suppliers in a secure manner to deter unauthorized access. To ensure there is no unauthorized access, Stadium shall establish a communication procedure between the each of the suppliers, personnel at the Authorized Location, and the Commission to properly control the shipping and receiving of all software and hardware components. Such procedures must include the following:

- Notification of pending shipments must be provided to the Commission by the Authorized Location;
- Certification by an independent test laboratory;

[1] Note: If the stamping machine is interfaced with a time clock such that the time on the stamping machine is kept accurate through the use of an independent automated update process, then this procedure is not required.

- 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 to ensure the Commission, or its designee, is present when an Authorized Location receives all hardware components. The shipping notification must include the following:
    - Name and address of the Supplier;
    - Description of shipment;
    - For hardware: serial number;
    - For software: software version and description of software;
    - Method of shipment; and
    - Expected date of delivery.

Stadium shall implement procedures for the maintenance and repair of the software and hardware components in accordance with the guidelines established by their suppliers and industry standards.

Location and Security

The Authorized Location provides a secure location within the Commonwealth for the placement, operation, and usage of wagering equipment, including Ticket Writer Stations, Kiosks, displays, and communications equipment. Stadium has submitted 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 includes the surveillance camera coverage and the money routes.

Any proposed changes and re-locations of wagering equipment will be submitted on subsequent floorplans in which the equipment is identified by location number(s). Wagering equipment has location numbers affixed to the outside and is clearly visible and readable by the CCTV. Stadium cleans out temporary files on hard disks drives and checks the following tasks on a scheduled basis:

- Clean out temporary files on hard disk drives;
- Hard disk space usage to ensure sufficient space is available for continued operations;

- All scheduled tasks are running correctly;
- Event logs for system, application, security, browser, DNS, and other errors; and
- UPS systems.

Stadium prevents persons from tampering with or interfering with the operation of any wagering or equipment through physical security controls. Security monitors for forced entry, evidence of any entry, and protection of circuit boards containing programs. Stadium ensures 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.

Installation

Testing is 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. Testing includes the following, as applicable:

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

Maintenance

Wagering equipment will be maintained and serviced as per the manufacturer's recommendations and software will be updated as necessary upon availability of updates or as recommended by developers.

Wagering equipment maintenance is independent of the sports betting function. Maintenance employees report irregularities to management independent of the sports betting function.

Whenever a wagering equipment utilizes a barcode or microchip reader, the reader will be tested at least annually by employees independent of the sports betting function to determine that it is correctly reading the barcode or microchip.

Malfunctions

Equipment will be regularly tested and monitored for malfunctions. Upon identification or knowledge of an equipment malfunction, the same must be investigated, documented, and resolved as soon as practicable. The following procedure must be followed upon identification of a malfunction:

- Disabling and powering down wagering equipment until repaired;
- Determination of the event causing the malfunction;
- Review of relevant records, reports, logs, surveillance records;
- Repair or replacement of the wagering equipment; and
- Verification of the integrity of the wagering equipment before restoring it to operation.

In the event of a communication malfunction occurring between the Sports Betting System and the wagering equipment which cannot be repaired immediately, Stadium will report the malfunction to the Commission in writing within five (5) days of the discovery. In the event that a malfunction is detected by the Commission, the wagering equipment will be disabled until such time that the malfunction has been repaired.

Removal, Retirement and/or Destruction

When not in use wagering equipment is stored in a location which is secure and only accessible by authorized personnel staff.

Stadium will notify the Commission in advance whenever a wavering machine will be moved to the secure location. The notification will 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.

Stadium performs the following procedures when removing wagering equipment or components from operation:

- For equipment or components that accept financial instruments:
    - Coordinate with the drop team to perform a final drop;
    - Collect final accounting information such as meter readings, drop and payouts;
    - Remove and/or secure associated equipment such as locks, card reader, or printer from the retired or removed component; and
    - Document removal, retirement, and/or destruction.
- For removal of software components:
    - Uninstall and/or return the software to IT; and
    - Document the removal.
- For all components:
    - Verify that unique identifiers, and descriptions of removed/retired components are recorded as part of the retirement documentation; and
    - Coordinate with the Accounting function to properly retire the component in the system records.

Stadium will seek authorization from the Commission before destroying any wagering equipment or components, and will conduct and document the following procedure upon approval:

- Describe the methods of destruction;
- Procure a witness or the surveillance of the destruction;
- List and describe all components destroyed; and
- Obtain the signatures of personnel(s) destroying the components attesting to destruction.

Commissioning, alteration, and de-commissioning of wagering equipment will be documented and must include the following:

- Identify and conduct the corresponding tests whenever wagering equipment is moved or relocated from their initial locations to new locations at the site.
- 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.

- Record the results of the tests, which include records signed by a representative from Stadium's designated function.
- 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.
- e. Ensure that all data collected in the Sports Betting System prior to de-commissioning wagering equipment.

Wagering equipment will not be used before the tests have been successfully completed and the information on the Sports Betting System has been verified as being correct.

Communications Technology

Before installing or permitting the installation of any communications technology, Stadium will notify the Commission of the location and number of each communications technology, and will obtain the approval of the Commission for each. Before Stadium accepts any wagers, written approval will be obtained from the Commission to accept such wagers.

As a condition to the granting of the privilege of having the communications technology, Stadium acknowledges that it 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. Stadium additionally understands and acknowledges that after any such removal, it 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.

Upon the request of either the Commission, Stadium 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 its operations.

Key Controls

Sensitive keys are those that either management or the Commission designates sensitive to Stadium's operation and therefore require strict control over storage, duplication, custody, issuance and return. Sensitive keys include the following:

- Unique identifier for each individual key;
- Key storage location;
- Number of keys made, duplicated, and destroyed; and
- Authorization and access.

Physical inventories of sensitive keys are conducted quarterly to ensure that the physical count and the access list count match. Stadium identifies the employee responsible for conducting the physical inventories of sensitive keys and which management employee has the authority to make changes, deletions and/or additions to the key access list. Stadium maintains safeguard for the use, access, and security of keys by documenting the following:

- Location of all sensitive key boxes and whether any of the boxes are portable or controlled by dual locks;
- Job titles which have authorized access to the sensitive key box key(s) and how they are issued and controlled;
- Sensitive key name, location, custodian and job titles authorized to sign out each sensitive key; and
- Location and custodian of duplicate sensitive keys.

Each sensitive key box is under constant surveillance coverage. Each box custodian will be issued a key access list noting authorized job titles that may access each key. Whenever two sensitive keys are required to access a controlled area, the keys will be independently issued to different employees.

Access to and return of keys are documented with the date, time, and signature or other unique identifier of the employee accessing or returning the key(s). At least two drop team employees are required to be present to access and return keys and at the time count room and other count keys are issued for the count.

Custody of all keys involved in the drop and count are maintained by personnel independent of the functions being dropped and counted. Any use of keys at times other than the scheduled drop and count receive authorization and are documented.

Emergency manual keys, such as an override key, for computerized, electronic, and alternative key systems are maintained in accordance with the following:

- 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.
- Date, time, and reason for access, is documented with the signatures of all participating persons signing out/in the emergency manual key(s).
- 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.
- 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).

Security and Surveillance

Authorized Location Security

Authorized Locations are designed to promote optimum security for sports betting. Stadium has provided the Commission a Security and Surveillance Plan and Procedures, attached hereto as an exhibit, for accepting wagers in any approved Authorized Location. Any changes to the security and surveillance plan will be approved by the Commission.

Identification Badges

Identification badges issued by the Commission are worn by Stadium or Authorized Location employees, officers and directors in a clearly visible location above the waist, while they are present within the Authorized Location.

Policy on Personnel Protection

Stadium ensures that all personnel are receiving an adequate level of protection with regard to both their safety and security, including:

- Personnel working remotely outside Authorized Location.

- Personnel working inside the Authorized Location areas with public access.

Prevent Wagering by Prohibited Players or Intoxicated and Impaired Persons

Stadium ensures a Prohibited Player or a player who is in a state of intoxication or is otherwise impaired is prohibited from participating in sports betting. Once aware that a Prohibited Player or an intoxicated or impaired person is in the Authorized Location, the employee will immediately notify security to remove them from the Authorized Location.

Closed Circuit Television (CCTV) Systems

Stadium maintains a CCTV System to monitor sports betting operations conducted within an Authorized Location. Stadium and the Commission have free access to the CCTV of the Authorized Location and its transmissions.

For operations at points of sales or satellites, the CCTV shall be maintained and operated from a secured location such as a locked cabinet. For operations at principal locations, the CCTV is maintained and operated from a secured location in which:

- Unauthorized entry is prevented;
- Access is limited to surveillance personnel and other authorized persons;
- Access logs are maintained;
- Equipment must have total override capability over all other satellite surveillance equipment; and
- Cameras are installed in a manner that prevents them from being readily obstructed, tampered with, or disabled.

The CCTV System will monitor and record:

- Activities occurring in the main cage with sufficient clarity to view cage and counter activities, and to confirm the amount of each cash transaction;
- Activities occurring at Kiosks and Ticket Writer Stations with sufficient clarity to view individuals performing the activities, including maintenance, drops or fills, and redemption of wager tickets, vouchers or credits;

- 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
- An accurate date and time stamp on recorded events; and
- A sufficient number of recording devices to record the views of all cameras and have the capacity to display all camera views on a monitor.

Recordings of sports betting operations are retained for at least ninety (90) days from the date of recording, unless Stadium 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 are copied and retained for a time period of not less than one year. To ensure proper documentation, logs are maintained and contain the following:

- Compliance with the storage, identification, and retention standards;
- Each malfunction and repair of the CCTV System; and
- Activities performed by surveillance personnel as required.

In the event of power loss to the CCTV System, an auxiliary or backup power source is available and capable of providing immediate restoration of power to the CCTV to ensure that surveillance personnel can observe all areas covered by dedicated cameras. During the period of time that the Authorized Location is open to the public, there will be adequate lighting and continued surveillance of the sports betting operations.

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

A periodic inspection of the CCTV Systems will be conducted. When a malfunction of the CCTV is discovered, the malfunction and necessary repairs are documented, and repairs will be initiated within seventy-two (72) hours of discovery. If a dedicated camera malfunctions, alternative security procedures, such as additional supervisors or security personnel, will be implemented immediately. The Commission will be notified of any

CCTV and/or camera(s) that have malfunctioned for more than twenty-four (24) hours and the alternative security measures being implemented.

Power Outages

Stadium's security personnel ensures that all players, employees and company assets are safeguarded against incidents that may occur during a power outage. Upon the occurrence of a power outage, security representatives are dispatched to the following areas:

- All cages, satellite cages and betting counters;
- Tops and bottoms of escalators, stairwells and elevator;
- Count room(s) if count(s) are in progress; and
- All other sensitive areas.

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

Player Account Management

Player Account Procedures

Stadium maintains procedures to address:

- Creation and use of Player Accounts, provided, that the 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.
- Maintenance of documents related to the establishment of Player Accounts.
- 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 Stadium at least five (5) days in advance to the effectiveness of the prohibition.
- Acceptance of wagers including, but not limited to:
    - Method of wagering communications; and
    - Player account transactions documentation.

Within an Authorized Location, Player accounts are established, maintained, and accounted for in one designated area. Stadium ensures Players provide all information requested on the registration form. All subsequent deposits/withdrawals and account adjustment transactions are accounted for through the same designated area.

Registration and Verification of Players

Players can initiate the creation of their wagering account online but will have to visit an authorized retail location to verify and complete their registration and wagering account creation.

To establish a wagering account, the system will collect the following mandatory information:

- Name;
- Date of birth;
- Physical address;
- E-mail address;
- Phone number; and
- Last four digits of social security number (if a resident of the United States)

Note: this information is treated as personal identifiable information (PII), thus it will be secured and transmitted in encrypted form to our identity verification and know your client (KYC) service provider for verification and final activation.

Stadium maintains an identity verification process as a part of its registration process, which, for bets placed online, includes the use of an independent Identity Verification Service Provider ("IVSP") to verify an individual's PII. Stadium provides to 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 Stadium or the Commission.

Stadium notifies the Commission of any changes to its verification procedures, or in the event there is a change of an IVSP. The verification procedures performed by Stadium are recorded, maintained and include the following information:

- If an IVSP performs the verification process, the third-party service provider's verification results and verification date.
- 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.
- Multi-sourced authentication used to verify the accuracy of the information provided for the player's date of birth and the physical address where the player resides.

The verification procedures contain identification methods to mitigate the risks of non-face-to-face transactions. The IVSP may require a player to provide additional information, copies of documents, in order to complete the registration process.

To complete and activate a wagering account, and before placing or accepting any bet, player must visit an authorized retail location. The following procedure will be followed, and information collected.

- An employee examines, in front of the person, player's valid (that is, current, non-expired) identification that may be any of the following:
  - driver's license;
  - passport; or
  - other picture identification credential normally acceptable as a means of identification when cashing checks.
- The employee then records or confirms the following on a printed form or directly in the system:
  - A description, document number and expiration of the identity credential examined;
  - A patron's valid driver's license is the preferred method for verifying the patron's identity. A passport, non- resident alien identification card, other government issued identification credential or another picture identification

credential normally acceptable as a means of identification when cashing checks, may also be used;
    - That player is not listed in a Prohibited Player list or a Self-Excluded listing;
    - The method used to verify player's identity and residence, to ensure the account has not been created using an anonymous or fictitious name. This includes recording the identification credential's number and description or making a copy thereof;
    - The date player's account with was established;
    - Player's name, physical address, and telephone number (; post office box numbers are not accepted for physical addresses);
    - Player's date of birth, gender and last four digits of the social security number (if player is a resident of the United States);
    - Player's initial deposit, if any; and
    - Player's assigned account number.

The teller or supervisor will locate the attestation function on the system whereby player will have to sign attesting to the following:

- The information that player is providing to the Company for registration is correct;
- That player has been informed, and accepts, that player is prohibited from allowing another person access or use of player account; and
- That player acknowledges that the activity reflected in a player's account and player's earnings may be disclosed to the Commission, the Puerto Rico Treasury Department, the Internal Revenue Service, and other federal or local government agencies.

All wagering accounts are established, maintained, and accounted for at the authorized retail location where the player completed his/her wagering account registration. Further, a record of each deposit, withdrawal, and adjustment created is maintained in the system.

The system will not allow bets unless an account is validated at an authorized retail location. Identification verification will be required as part of the application process.

Stadium maintains procedures for handling the unsuccessful verification of the information provided by an individual who is registering as a player. Stadium records and maintains the following information:

- Unique player ID and player name;
- Date the account was suspended from further sports betting by the player;
- Date the account was closed;
- Amount of winnings retained which were attributable to the player; and
- Balance of amount refunded to the player.

Protection of Player Accounts

Stadium prohibits players from establishing more than one active Player account. Stadium identifies the player authorized to use the Player account and prevents the unauthorized access to, or use of, the account by any individual other than the player for whom the account is established.

Player's must set up a username and password for his/her wagering account. The password must be at least eight (8) characters in length, include an uppercase letter and a special character. Any Player account is automatically locked-out after three failed access attempts in a thirty-minute period. A multi-factor authentication process is employed for the account to be unlocked or to recover or reset a password or username. Player accounts will be immediately suspended, and Player's identification immediately re-verified upon reasonable suspicion that the identification has been compromised.

Stadium may require a player to change or update account information at any time, including the player's username and password. A player may make such changes and updates by visiting an Authorized Location of Stadium or calling its customer service line.

Multi-factor authentication is required before allowing a player to change their password, access/update PII, transfer funds, or to remove a player from Stadium's Self-Exclusion list.

Communication via e-mail is a component of this process .As such, solutions in place for use in the event that a player no longer has access to the e-mail address on record. In any such case, the player may use multi-factor authentication or visit an Authorized Location to regain access to his or her account.

A wagering account may be suspended if the Company has a suspicion or sufficient reason to believe that the account has been compromised or used to commit fraud or other illegal activity.

Personally Identifiable Information (PII) Security

PII is considered a critical asset for the purposes of risk assessment. This includes, but is not limited to:

- The amount of money credited to, debited from, or present in any particular player account;
- The amount of money wagered by a particular player on any Sports Event or Special Event;
- The account number and authentication credentials that identify the player; and
- The name, address, and other information in the possession of Stadium that would identify the player to anyone other than the Commission or Stadium.

Stadium maintains protocols to ensure the security of PII, as required by the Commission, which include, but are not limited to, the following:

- From time to time, the IT Manager will designate and identify of one or more employees having primary responsibility for the design, implementation and ongoing evaluation of such procedures and practices.
- Stadium identifies the following:
    - The nature and scope of all PII collected;
    - The purpose and legal basis for PII collection including, where required by the Commission, the “legitimate interest” pursued by Stadium;
    - The locations in which the PII is stored, and the storage devices on which the PII is recorded for purposes of storage or transfer;

- Period in which the PII is stored, or, if no period can be possibly set, the criteria used to set;
- 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; and
- The communication to the Commission in the event Stadium determines that a breach of data security has occurred shall be made by the IT Manager and the Chief Operations Officer within 24 hours.

In order to request the following from Stadium, players can visit an authorized location as well Stadium's central office, or call Stadium's call center:

- Confirmation that their PII is being processed;
- Access to a copy of their PII as well as any other information about the PII processing;
- Any updates to their PII; and
- That their PII is erased and/or to impose restrictions on processing of PII.

Stadium records and processes requests from players, including maintaining records of requests, and providing reasons to the player when such requests are denied or rejected. When Stadium does not intend to comply with the request, the player is given a reason and is also provided with the necessary information on the possibility to file a complaint with the Commission.

Where required by the Commission and upon player's request, Stadium will forward to the player the PII that Stadium has received from such 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:

- PII which the player has provided to Stadium, or PII which is processed by automated means and
- Where the basis for processing PII is given consent, or that the data is being processed to fulfil a contract or steps preparatory to a contract.

Where required by the Commission, the player has the right to object to PII processing and/or withdraw consent, if:

- There exist legitimate interests or the performance of a task in the public interest or in the exercise of official authority;
- The PII is being used in direct marketing; or
- The PII is being used for scientific or historical research purposes.

Stadium complies with requests from players to have their PII erased and/or to prevent or restrict processing of their PII, including, in the following circumstances:

- No longer necessary in relation to the purpose for which it was originally collected/processed;
- Player withdraws consent;
- Player objects to the PII processing and there is no overriding legitimate interest for continuing the processing;
- PII was unlawfully processed; or
- PII has to be erased in order to comply with a legal obligation.

Where applicable, the player is provided with information on Stadium's use of automated decision-making, including profiling. This includes:

- Sufficient insight into the logic of the automated decision-making.
- Significance and consequences of such processing for the player.
- 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.

Where prohibited by the Commission, Stadium will not utilize solely automated decision-making which:

- Produces legal effects such as those which result in the player being subjected to surveillance by a competent authority; or
- Significantly affects the player in a similar manner.

Payment Service Providers

Stadium, or the Payment Service Provider (PSP) used to conduct transactions with financial institutions, undergoes an annual audit against common cybersecurity and information security principles in relation to the provision and use of payment services. Stadium may leverage the results of prior audits conducted by accredited vendors within the current audit period, against standards such as the Payment Card Industry Data Security Standards (PCI-DSS) or equivalent. Such leveraging is noted in the audit report.

Stadium or the PSP protects payment types used in the system from fraudulent use. The actions performed to ensure such protection include the following:

- Collection of sensitive information directly related to deposit/withdrawal transactions is limited to only the information strictly needed for the transaction;
- Stadium or PSP verifies the protection of the sensitive information directly related to each deposit/withdrawal transaction;
- Any communication channels between Stadium and the PSP conveying deposit/withdrawal details are encrypted and protected against interception; and
- Financial transactions are reconciled between Stadium and the PSP daily, including:
    - Calculating amounts paid to or received from a player; and
    - Assuring the match of ownership between the payment type holder and the Player account holder so as to avoid fraud and money laundering.

Player Funds Maintenance

Player Funds Protection

Funds held within Player accounts are not used as security by Stadium for any financial transactions and are considered as critical assets for the purposes of risk assessment.

Financial Transactions

Prior to the player making a deposit or withdrawal from an account, Stadium will verify the player's wagering account, the player's identity, and the availability of funds. The

player will be provided confirmation/denial of every deposit/withdrawal transaction initiated, including:

- The type of transaction (deposit/withdrawal);
- The transaction value; and
- For denied transactions, a reason as to why the transaction did not complete as initiated.

A record of each deposit/withdrawal/adjustment is created and maintained that details the following information:

- Account number and player name;
- The type of transaction (e.g., deposit, withdrawal, adjustment);
- The date and time of the transaction;
- Unique transaction identification number;
- The amount of transaction;
- The total account balance before/after transaction;
- The total amount of fees paid for the transaction, if applicable;
- User identification of employee or unique wagering equipment ID which handled the transaction, if applicable;
- Method of deposit or withdrawal;
- Deposit authorization number;
- Relevant location information;
- Player signature for withdrawals, unless a secured method of access is utilized; and
- For adjustments to the account, the reason for the adjustment.

Stadium's employees shall be trained to confirm that the player deposit and withdrawal forms contain the sequence of the required signatures, including the cashier's signature, attesting to the accuracy of the information contained. Each ticket writer is assigned a unique date/time stamp used solely at the ticket writer's assigned window. Payouts of $3,000 or more, or those exceeding any tax reporting threshold, requires the supervisor to enter an approval code and to sign the wager ticket. Deposits, withdrawals, or payouts of $10,000 or more also requires the supervisor to enter an approval code and to sign the wager ticket/voucher.

All player deposit and withdrawal transactions at the cage are recorded on a cage accountability form on a per-shift basis.

The information for deposits/withdrawals above should be included on a receipt as follows:

- A manual deposit/withdrawal is evidenced by at least a 2-part document, with one part remaining in the cashier's area and the other part given to the player. In addition, the document must include the same document number on all copies and the signature of the employee handling the transaction; or (not applicable if an electronic receipt is utilized)
- A computerized deposit/withdrawal is evidenced through an electronic receipt which is to be provided to the player.

Identification verification is required upon withdrawal by a player from a wagering account. Players are not allowed to transfer funds to any other account, unless the other account is verified to be controlled by the player.

Only Supervisors and upper management employees have access to adjust wagering accounts.

A printed statement of the player's wagering account activity is available upon written request from the player or if player visits an authorized retail location. The printed statement is a record of the following:

- account number;
- name of player registered to the account
- beginning balance;
- list of all transactions which includes the following:
    - date and time;
    - amount of transaction;
    - transaction type (e.g., deposit, withdrawal, etc.); and
    - player(s)/employee(s) who initiated and authorized the transaction;
- totals by credits and by debits; and

- ending balance.

Stadium will collect and maintain the following information:

- A detailed record by Player account and date of all funds on deposit;
- A current balance of all player deposits that are in the cage/count room inventory or accountability; and
- Reconciliation of the current balance with the deposits and withdrawals. at least on a daily basis.

Stadium may withhold incorrectly deposited amounts from any deposit or prize. If a player withdraws funds that were incorrectly credited to their Player Account, Stadium may use internal and external attorneys to seek relief under any remedies available pursuant to Puerto Rico laws.

Deposits

Stadium documents 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.

For its expected operations upon their commencement, Stadium will only be accepting deposits made in person, whether made with a cashier at the counter of an authorized location or at a kiosk within the limits established herein.

A cashier accepting a deposit will use the World Till to enter the customer's account ID, find the customer's account, and verify the customer's account in the Sports Betting System. If the account is found, the context is set (Monitored Customer panel), and the customer's details are shown in the main screen. At such point, the cashier will enter the amount of the deposit, which can be registered as cash and/or chips received. The cashier will press the Deposit button (F6) and the transaction shall be processed, having the customer's account be credited when the transaction is completed. Upon completion, two receipts are printed, one for the customer and one for the cashier. The amount to collect from the customer is shown in the Sub-Total panel and the transaction added to the Transaction List. The cashier will press Session End (F12) to finish the procedure.

Deposits of $10,000 or more also requires the supervisor to enter an approval code and to sign the wager ticket/voucher.

As established by the MICS, the routing procedures for deposits by mail require that the mail deposits are received by a function independent of the Sports Betting Function. Therefore, they shall be received by the Accounting Function.

Withdrawals

Customers can make cash withdrawals from their sportsbook wagering accounts directly at a cashier window (World Till). To do this, the customer must first make the request using the wagering account to obtain a withdrawal code. This code is then given to the cashier as part of the withdrawal process.

The basic steps employed by Stadium are as follows:

1. Log in to the wagering account
2. Clicks Withdraw or the Cashier command
3. Next, the customer picks the Withdrawal option under Cash In Shop
4. The customer enters the amount to withdraw and once the transaction is processed the system issues a claim number (authorization code).
    - Withdrawals of $3,000 or more, or those exceeding any tax reporting threshold, require the supervisor to enter an approval code and to sign the wager ticket.
    - Additionally, the system has a mechanism that can detect and prevent any player-initiated withdrawal activity that would result in a negative balance of a Player account.
5. When a withdrawal is requested, an email/SMS notification is sent containing the authorization code, which can also be used as part of the claiming process at the cashier window.
6. When a code is generated, the request is authorized but not yet processed (paid out), so the requested amount is placed in “Locked Funds”. The Total Balance as yet remains unchanged, but the locked amount is deducted from the Trading Balance (i.e. the customer cannot use the locked funds for game play).
7. Once the cashier begins the payout procedure selecting Wagering Account Withdraw, this will open the Wagering Account Withdraw screen. The cashier shall enter the customer’s account ID and press find and the account is verified by the system.

- For this step, Stadium's employees ensure that direct access to a Player account to withdraw funds is restricted to the player who owns the account and who is confirmed to be the owner by using positive player identification methods.
- Additionally, indirect access to a Player account to withdraw funds involves assisted access by a member of the Customer Service function, who will ensure that the person is accurately identified as the owner of the account.

8. If the account is found, the context is set (Monitored Customer panel), and the customer's details are shown in the main screen.

9. At this point, the customer tells the cashier the requested amount and the authorization code and the cashier enters these values and presses Pay in Cash. The values must match or the system will generate an error message.

10. If the authorized amount and correct code are entered, the withdrawal transaction is processed.

11. Two receipts are printed, one for the customer and one for the cashier.

12. The amount to pay the customer is shown in the Sub-Total panel and the transaction added to the Transaction List.

13. The cashier shall press Session End (F12) to finish the procedure.

Electronic Funds Transfers (EFT)

Where financial transactions are allowed through the Electronic Funds Transfers (EFT), the Company have security measures and controls to prevent EFT fraud. A failed EFT attempt will 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 Company will:

a. Temporarily block player's wagering 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
b. Suspend player's wagering account after five (5) additional consecutive-failed ACH attempts within a ten (10) minute period.

The Company may require players to provide additional information, provide copies of documents, or appear in person at an authorized retail 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 wagering account transactions.

Adjustments

Stadium may withhold incorrectly deposited amounts from any deposit or prize or seek recovery if a player withdraws funds that the Company has reason to believe were incorrectly credited to their wagering account.

Stadium ensures that only authorized adjustments are made to Player accounts by following the below controls:

- All adjustments under $500 are periodically reviewed by supervisory personnel.
- All other adjustments are authorized by supervisory personnel prior to being entered.
- Documentation of the job titles of supervisory personnel authorized to perform this function and specify which evidence of supervisory authorization is to be recorded and maintained.

On a daily basis, supervisory personnel may authorize multiple transactions. Evidence of supervisory authorization for multiple transactions is recorded and maintained. The Main Cage Manager shall be the only employee with authority to authorize multiple transactions rather than authorizing each individual transaction. The system shall be able to issue reports identifying which transactions were authorized through a multiple authorization and the Compliance Manager shall review and analyze such reports on at least a weekly basis.

Account Closure

Stadium permits an individual, group of individuals, or entity that places wagers to terminate the account at any time and for any reason and without penalty. A player is 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.

Players will not be encouraged or induced to keep their accounts open following their request to close their account. Stadium offers a readily accessible method for a player to close his or her account at any time. The account closure process will commence immediately upon receipt of the account closure request.

The account may remain in pending closure status if there are outstanding confirmed wagers. The account closure process will result in the account being closed after all wagers have been settled. Any balance remaining in a Player account closed by a player will be refunded within five (5) business days, provided that Stadium acknowledges that the funds have cleared.

Dormant and Closed Accounts

Access to dormant and closed account information is restricted to personnel that require access and are so authorized by management. Initially, the Main Cage Manager shall have access to such accounts. Any other personnel that require access must be approved by the Chief Financial Officer and General Counsel. Such access request and authorization must be made in writing and the system shall keep track of the accounts accessed by any authorized employee.

Reports and Information Storage

Reporting Requirements

Adequate documentation of all pertinent sports book information is generated by the Sports Betting System. The Sports Betting System generates the information needed to compile the following reports on demand, on a daily basis and a monthly basis as deemed necessary:

- Wager Summary Reports- summary of wagers on events, including those in process and completed.
- Win Summary Reports- 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.
- Potential Payout Reports- 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.

- Account Financial Transaction Reports- the unique transaction identifier, the date and time of the transaction and the amount of each deposit, withdrawal, or adjustment during the period, by Player Account and in total.
- Account Wagering Reports- 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.
- Ticket Wagering Reports- 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.
- Winning Wager Ticket Redemption Reports- 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.
- Unredeemed Winning Wager Ticket Reports- 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.
- Voucher Issuance Reports- 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.
- Voucher Redemption Reports- 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.
- Unredeemed Voucher Reports- the unique voucher identifier, the date and time of issuance, the expiration date, and the amount of each voucher that has not been paid.
- Player Wagering Account Balance Reports- 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.
- Event Results Reports- 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.
- Sports Betting Operator Liability Reports- each amount listed under the Regulations for “Operator Reserves” and its total amount.

- Adjusted Gross Revenue Reports- the amounts for wagers, prizes, voids, cancellations, takeout or fees, and other expenses.
- Sports Betting Statistical Reports- 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.
- Voluntary Exclusion Reports- the total number of persons that requested to exclude themselves from sports betting including their names.
- Involuntary Exclusion Reports- a list of names of persons whom Stadium has excluded from sports betting including the reasons why the person was excluded.

The reports are distinguished by type and status where applicable and be produced in an approved format.

Exception Reports

The Sports Betting System can generate exception reports for significant events or alternations.

Significant events and alternations that will be tracked include, but are not limited to the following:

a. Failed login attempts exceeding 3 number of attempts, including IP Address.
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.
d. Large wins (single and aggregate over a 24-hour time period) in excess of $10,000 or any other amount specified by the Commission, including wager information;
e. Large wagers (single and aggregate over a 24-hour time period) in excess of $10,000 or any other amount specified by the Commission, including wager information;
f. Large financial transactions (single and aggregate over a 24-hour time period) in excess of $10,000 or any other amount 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.
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.
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 wagering account balance;
q. Changes made to PII and sensitive information recorded in a player wagering account;
r. Deactivation of a player wagering account;
s. A negative player wagering account balance;
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;

The above Exception reports produced by the Sports Betting System will include, at a minimum, the following:

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.

Exception reports are reviewed daily for propriety of transactions and unusual occurrences. The review is 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.

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

The following employee(s) are responsible for reviewing the exception reports:
Privacy and Anti-money Laundering Director

Evidence of this review (e.g., log, checklist, notation on reports) is maintained for 18 months following the completion of the review. The evidence gathered will include the following information:

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.

IT Personnel who review the logs are independent of the system administration and user access administration and do not have system access to perform any administrative functions in the systems for which the logs are being reviewed.

Electronic Storage of Information

Stadium maintains reports and other documents/records that are written to an electronic document retention system in a portable document format (PDF), or scanned to an electronic document retention system. As part of its internal controls, the following items must be met:

- If scanned, documentation will 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 provides 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.
- On a quarterly basis, internal audit will review a minimum of 20 documents added to the electronic document retention system. The review will assess whether:
    - 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.
    - The documents are readable and version control is functioning properly.
    - The indexing is accurate.
    - User access to add or modify documents is set to an appropriate level of access to administer the electronic document retention system, and terminated employees do not have active user accounts on the system.
    - The event recording and reporting is functioning as designed and the logs are being reviewed by the appropriate personnel regularly.
    - 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 another unforeseen event.

Evidence of the review is maintained for five (5) years. The evidence includes the following items:

- The date and time of review;
- The name and title of person performing the review;
- The document records reviewed; and
- Any exceptions, including follow-up and resolution of such exceptions.

Bank Secrecy Act (BSA) Compliance

Transactions in Excess of $10,000

Stadium reports cash transactions in excess of $10,000 that appear to be transacted to avoid filing requirements of the Bank Secrecy Act, Title 31. Stadium is obligated to comply with all applicable local and federal regulations.

Stadium completes and files Currency Transaction Report (CTR) with the Financial Crimes Enforcement Network (FinCEN) of each or multiple of the following types of cash transactions:

- A wager of $10,000 or more;
- A player account deposit of $10,000 or more;
- A payout of $10,000 or more on a winning wager; or
- A player account withdrawal of $10,000 or more.

Each type of transaction is aggregated separately in order to determine that the reporting threshold is met. Stadium monitors all transactions to ensure players are not circumventing these requirements. Thus, prior to accepting any straight or fixed odds (nonpari-mutuel) bet in excess of $10,000 or making a pay out in excess of $10,000 on a nonpari-mutuel winning bet and before concluding any transaction where a CTR is required to be filed, Stadium will obtain and record the following player information:

- Legal name;
- Date of birth;
- Obtain or reasonably attempt to obtain the player's permanent residential address (a post office box is not acceptable);
- Social Security number or equivalent for a foreign player such as a passport or taxpayer identification number;

- obtain one of the following identification credentials from the patron, which must be valid (that is, current, non-expired):
  - driver's license;
  - passport;
  - non-residential alien identification card
  - other reliable government issue identification credentials; or
  - other reliable picture identification credentials normally accepted as a means of identification when cashing checks.
- examine the identification credentials obtained to verify the player's name, and to the extent possible, to verify the accuracy of the information obtained.

The information may 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. If the player is unable to provide an acceptable form of identification, the transaction will 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.

After accepting a straight or fixed odds (nonpari-mutuel) bet in excess of $10,000 or making a payout in excess of $10,000 on a nonpari-mutuel winning bet, Stadium will record it in and maintain records that include:

- Player's legal name and, if applicable, the agent's name;
- Player's date of birth and, if applicable, the agent's date of birth;
- Player's address and, if applicable, the agent's address;
- Player's social security number and, if applicable, the agent's social security number;
- A description including any document number of the identification credential examined (or credential information on file for known patrons) and, if applicable, for the agent;
- The amount of the transaction;

- Station number;
- Ticket Writer number or other identification of the location where the transaction occurred;
- The time and date of the transaction;
- Names and signatures of Stadium employees accepting or approving transaction; and
- Where possible, a surveillance photo of the player. The photo will 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 a written explanation that there was no photograph taken because it is an after the fact CTR.

Any CTRs prepared by sports betting personnel must be submitted to the Accounting Function within 24 hours.

CTRs are filed with FinCEN within 15 days following the day on which the reportable transaction occurred. Stadium will file an amended report if it obtains information to correct or complete a previously submitted report, and the amended report will reference to the previously submitted report. Stadium will 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, all communication will be sent using an encryption process of encoding messages.

Before completing a transaction with a player that, when aggregated with others, totals more than $10,000 during any operational day, Stadium will complete a Multiple Transactions Log (MTL) with identification and record keeping requirements described above. One log will be maintained for the Company, for each designated 24-hour period. A log will be completed for each 24-hour period regardless of whether any straight or fixed odds bets occurred. Multiple transactions, of the same type or category, will 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.

Each log entry in a Multiple Transaction Log will be made by the ticket writer/teller, a shift supervisor, or manager accepting or approving the bet, immediately after accepting the bet, and will include the following:

- 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, the employee completing the log will attach to it a written explanation of why there is no photo and will procure a description of the player (or suspected agent), which may include identifiers such as age, sex, race, eye color, hair, weight, height and attire; if the person is present when the wager is accepted;
- player's legal name (or suspected agent's name), if known;
- player's date of birth, if known;
- player's residential address, if known (a post office box is not acceptable);
- player's Social Security number or equivalent for a foreign player such as a passport or taxpayer identification number;
- window number or other identification of the location where the wager occurred;
- time and date of the wager;
- dollar amount of the wager; and
- signature or electronic signature of person accepting or approving the wager.

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.

Stadium will not knowingly allow, and will 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. Stadium will not encourage or instruct the player to structure or attempt to structure transactions. This does not prohibit Stadium from informing a player of the regulatory requirements imposed upon the License, including the definition of structured transactions. Within 24 hours after the end of a designated 24-hour period, MTLs created are submitted to the Accounting/Compliance function.

Anti-Money Laundering (AML) Compliance

AML Compliance Policy

Stadium maintains a comprehensive and robust AML compliance policy that is risk-based and adequately addresses the risks posed by sports betting for the potential of money laundering and terrorist financing. The AML compliance policy provides for:

- Internal controls- ensure ongoing compliance with AML regulations and standards observed by the Commission.
- Training- current 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.
- AML Officer- assigned individual responsible for AML matters including reporting unusual or suspicious transactions and a clear procedure for the review and implementation of any Compliance Manager recommendations or reports.
- Stadium has established a suspicious activity compliance committee who meets periodically for assessment of Suspicious Activity Reports (SARs) prepared for determination of filing.
- Monitoring Player accounts for opening and closing in short time frames and for deposits and withdrawals without associated wagering transactions.
- Aggregate transactions over a defined period may require further due diligence checks and may be reportable if they exceed the threshold prescribed by the Commission.
- Internal testing for compliance with the requirements of the sports betting and AML law.
- Integrating and sharing data as appropriate and feasible among:

        - Different parts of the Authorized Location;
        - Other operators;
        - Other entities providing sports betting services; and
        - Affiliates in other jurisdictions.
    - 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.
    - High risk or politically exposed persons (PEPs) are identified so that appropriate sign-off is obtained for transactions involving those persons.
    - Implementation of such measures as are necessary to assist law enforcement or regulatory authorities in the Commonwealth with any investigations or enabling those authorities to freeze or seize assets, as permitted by law.
    - Use of automated data processing systems to monitor the variety, frequency and volume of transactions.
    - Using all available information to determine:
        - Verification of the full name, date of birth, and residential address;
        - Occurrence of unusual or suspicious transactions; and
        - Whether a Suspicious Activity Report (SAR) needs to be filed.
    - 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 by the Compliance Manager.

AML Risk Assessment

Stadium conducts a risk assessment to identify any areas of its sports betting operations at risk for money laundering and the AML procedures specify the measures to address those risks. The risk assessment covers risks involving:

- Players:
    - Sources of wealth or income commensurate with their sports betting activity;
    - Provided personal, financial or business information that can be readily verified;

        - Fiduciary obligations that may create a risk of misappropriation of funds;
        - Is associated with individuals or entities known to be connected to the illicit activity;
        - Bankruptcy;
        - Prior history of criminal or dishonest conduct; and
        - Politically exposed persons (PEPs).
    - Products and services offered by or on behalf Stadium:
    - Employees in the proper performance of their functions and duties and as a voluntary or involuntary part of any AML scheme;
    - Use of foreign holding accounts where funds are held in a foreign jurisdiction for use in an Authorized Location in the Commonwealth;
    - Use of third-party marketing agents;
    - Ownership structures and integrity of intermediaries and associated businesses;
    - Criminal activities and proceeds of crime generated domestically as well as abroad but laundered domestically;
    - Financial services offered by Stadium or by an intermediary; and
    - Use of wagering equipment that accepts cash.

AML Compliance Manager

Stadium has, at all times, a Compliance Manager to assure day-to-day compliance and to be responsible for all areas of AML. The Compliance Manager shall be:

- Adequately trained to carry out the role, including reporting unusual or suspicious transactions;
- Knowledgeable of the relevant AML requirements;
- Available to other employees to consult on AML related issues as they arise;
- Knowledgeable of Stadium products, services, player base, and particular AML risk areas;
- Have appropriate authority and resources to implement Stadium's AML policies; and
- Responsible for ensuring that training is provided to:
    - Those engaged in the sports betting operation;
    - All employees with cash or credit handling responsibilities;

- Surveillance employees;
- Employees in the accounts function;
- Senior management; and
- Employees responsible for marketing or hosting high value players.

AML Program Violation

Stadium will notify the Commission within 24 hours upon discovery of any material violation or non-compliance with the AML compliance program, policies, and procedures, AML laws or regulations.

Accounting and Auditing Procedures

Accounting Controls

Stadium safeguards assets and ensure the regulations for "Financial and Compliance Auditing" are met including accounting controls which provide reasonable assurance that:

- Transactions or financial events pertaining to the revenues and expenses are:
  - Executed in accordance with Stadium's authorization protocols;
  - 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
  - Recorded to permit proper and timely reporting and calculation of proceeds and to maintain accountability for assets.
- Access to Stadium's facility and components in accordance Stadium's authorization protocols.
- The recorded accountability for assets is compared with actual assets at least annually and appropriate action is taken with regard to a discrepancy.
- Procedures are submitted that detail the reconciliation of assets and records contained in a Ticket Writer Station's drawer, Kiosk, and Sports Betting System.

Internal Audit Program

Internal audit activities are conducted in a manner that permits objective evaluation of areas examined.

Internal Audit Compliance Checklists will be 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 rules, regulations, and the MICS.

Audit reports will be maintained for a minimum of five (5) years and shall be made available to the Commission upon request. Such audit reports shall include the following information:

- Audit objectives;
- Audit procedures and scope, which include the following:
  - Whether the test was performed by inquiry, observation or examination;
  - The scope of each observation, review and test including the sample sizes and dates tested; and
  - 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 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.
- 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 will 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 will be reported. Non-sports betting related findings will not be included;
- Recommendations, if applicable. All recommendations are discussed with management prior to the report being submitted to the Commission;
- Observations. Exceptions noted that are not internal controls violations but relate to sports betting operations must be included; and

- Management's response. This includes 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.

The internal audit report is delivered to management, the audit committee, the Commission upon request, or any other entity as determined by Stadium.

All material instances of noncompliance identified by internal audit work will be investigated and resolved, and the results shall be documented and reported to the Commission.

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.

Documentation (e.g., log, checklist, notation on reports, and tapes attached to original documents) will be maintained to demonstrate 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 the Commission's MICS, including all instances of noncompliance.