ORDINANCE SPA/MF No. 722/2024

Establishes the technical and security requirements of betting systems, as well as their sports betting and online gaming platforms, to be used by fixed-odds lottery operators, as provided for in Law No. 13,756, of December 12, 2018, and Law No. 14,790, of December 29, 2023.

THE SECRETARY OF PRIZES AND BETS OF THE MINISTRY OF FINANCE, in the exercise of the powers conferred by Article 55, item I, paragraph "d", of Annex I of Decree No. 11,907, of January 30, 2024, and in view of the provisions of Article 29, paragraph 3, of Law No. 13,756, of December 12, 2018, in Article 7, paragraph 1, item VII, of Law No. 14,790, of December 29, 2023, and in Article 6, item V, of Normative Ordinance No. 1,330, of October 26, 2023, resolves:

CHAPTER I – PRELIMINARY PROVISIONS

Article 1. This Ordinance establishes the technical and security requirements of betting systems, as well as their sports betting and online gaming platforms, to be used by fixed-odds betting lottery operators, as provided for in Law No. 13,756, of December 12, 2018, and Law No. 14,790, of 29 December 2023.

Article 2. For the purposes of this Ordinance, the following shall be considered:

I – betting system: computerized system managed and made available by operators to bettors that enables the registration of bettors, the management of their virtual wallets and other functionalities necessary for the management, operation and commercialization of fixed-odds bets;

II – betting platform: electronic channel integrated with the betting system used to offer sports betting and online games to bettors.

III – certifying entity: legal entity with operational capacity recognized by the Ministry of Finance to test and certify equipment, programs, instruments and devices that comprise betting systems, live game studios and online games used by fixed-odds lottery operators, subject to the technical requirements established in a specific regulation;

IV – data center: place where the operating agent's computer systems are concentrated, such as the data storage system;

V – information technology continuity plan: plan that covers the strategies necessary for the continuity of essential information technology services, such as contingency, continuity and recovery;

VI – critical component: any component in which a failure or compromise may lead to the loss of the bettor's rights, loss of revenues of the Union or legal recipients, impediment or difficulties of access by the regulator to operational information, occurrence of

unauthorized access to the data of the betting system, or non-compliance with the rules that regulate the operation of fixed-odds betting in the country; and

VII – betting terminal: device made available by the operating agent in which the bettor can place bets in the physical modality.

CHAPTER II – TECHNICAL REQUIREMENTS

Article 3. The betting systems, integrated by sports betting and online gaming platforms, used by the operating agents to operate the lottery modality of fixed-odds betting shall observe and implement the technical requirements established in this Ordinance and its Annexes.

Article 4. Operating agents shall maintain the betting system and the respective data in data centers located in Brazilian territory, in compliance with the provisions of Law No. 13,709, of August 14, 2018.

§1 The systems and data referred to in this Article of this article may be located outside the national territory, in countries that have an International Legal Cooperation Agreement with Brazil, in civil and criminal matters jointly, provided that item VIII of the Article 33 of Law No. 13,709, of 2018, is observed, and the following requirements are cumulatively met:

I – the data subject shall authorize, in a specific and prior manner, the international transfer of his/her personal data, and the operating agent shall provide clear information as to the purpose of the operation;

II – the responsible technical area of the Ministry of Finance shall have secure and unrestricted access, remotely and in person, to the systems, platforms and data of the operation;

III – the operating agent shall replicate, in Brazil, its database and information, which will be updated continuously, ensuring that all instances of the database have the same content, and that they are periodically tested; and

IV – the operating agent shall present an Information Technology business continuity plan, in the event of the occurrence of critical situations that may jeopardize the operation and data, containing, at least:

a) mapping of probable loss scenarios;
b) risk identification, analysis and assessment;
c) prevention and mitigation actions; and
d) designation of responsible persons.

§2. The data center used must be ISO 27001 certified.

Article 5. The electronic channels used by the operating agent to offer fixed-odds bets in a virtual environment must use "bet.br" domain registration, according to specific regulations.

CHAPTER III – CERTIFICATION AND ASSESSMENT REPORT FOR CERTIFICATION

Article 6. Operating agents must maintain the betting systems, which include sports betting and online gaming platforms, certified by a certifying entity whose operational capacity has been recognized by the Secretariat of Prizes and Betting of the Ministry of Finance, under the terms of Ordinance MF/SPA No. 300, of February 23, 2024.

§1. The certificates issued by the certifying body must attest that the betting systems, including sports betting and online gaming platforms, are in full compliance with the technical requirements defined in Annexes I, II and III of this Ordinance, including in relation to the integration between their modules and platforms.

§2. In situations where the modules and platforms of the betting systems used by the operating agent do not have the same compilation version and the same supplier, it will be mandatory to verify the integration between them by the certifying entities whose technical capacity has been recognized by the Ministry of Finance.

§3. The betting systems, including the platforms referred to in this Article must remain with valid certificates throughout the duration of the authorization granted.

§4. The certificates issued by the certifying body for betting systems will include sports betting and online gaming platforms and must be revalidated annually, and whenever there is inclusion, alteration, and exclusion of critical components.

§5. The certificate revalidated under the terms of § 4 must be forwarded to the Secretariat of Prizes and Betting of the Ministry of Finance within 5 business days after the issuance.

Article 7. The certificates must be issued specifically for Brazil by the certifying entities authorized by the Secretariat of Prizes and Betting of the Ministry of Finance, under the terms of Ordinance MF/SPA No. 300, of February 23, 2024.

Article 8. The operating agents shall submit, within 90 days after the publication of the authorization act by the Secretariat of Prizes and Betting of the Ministry of Finance, an evaluation report for certification of the technical requirements defined in Annex IV of this Ordinance issued by a certifying entity whose operational capacity has been recognized by the Secretariat of Prizes and Bets of the Ministry of Finance.

Sole paragraph. The evaluation reports for certification issued by the certifying body for betting systems and for sports betting and online gaming platforms must be revalidated annually.

CHAPTER IV – SUPERVISION AND INSPECTION

Article 9. The activities of supervision and inspection of betting systems, which include sports betting and online gaming platforms, will be regulated in specific regulations of the Secretariat of Prizes and Betting of the Ministry of Finance, respecting the competences of other governmental and consumer protection bodies and entities.

Sole paragraph. For the purpose provided for in this Article, the operating agent shall, at any time, grant full access to the betting systems to the units and inspection agents of the Secretariat of Prizes and Betting of the Ministry of Finance.

Article 10. The operating agents must forward to the Secretariat of Prizes and Betting of the Ministry of Finance the data related to bets, bettors, bettors' wallets, legal destinations and other information about their operation, according to the periodicity and format established in the SIGAP Manual, available on the https://www.gov.br/fazenda/pt-br/composicao/orgaos/secretaria-de-premios-e-apostas website.

Sole paragraph. Without prejudice to the provisions of this Article, the Secretariat of Prizes and Betting of the Ministry of Finance may, at any time, request additional information from the operator.

Article 11. The betting systems, including its sports betting and online gaming platforms, will be subjected to inspection procedures, as requested by the Secretariat of Prizes and Betting of the Ministry of Finance.

CHAPTER V – BETTING TERMINALS

Article 12. Operating agents with certified betting systems, when authorized, may offer bets that have as their object real sports-themed events, in physical mode, through betting terminals.

Sole paragraph. Fixed odds bets that have as their object online gambling events can only be offered in a virtual environment.

Article 13. Betting terminals must always be connected and integrated with the operator's betting system, observing the technical requirements established in Annexes I and II of this Ordinance.

Sole paragraph. Bets placed on betting terminals will always be preceded by the identification procedures referred to in Article 23 of Law No. 14,790, of 2023, and will comply with all other rules for placing bets in virtual media, including those related to payment transactions, according to specific regulations of the Secretariat of Prizes and Betting of the Ministry of Finance.

CHAPTER VI – ONLINE GAMES

Article 14. The online games to be offered by the operating agents must have a multiplication factor of the amount bet that defines the amount to be received by the bettor, in case of prize, at the time of placing the bet, for each unit of national currency

bet, whose result is determined by the outcome of a random future event, from a random number generator, of symbols, figures, or objects defined in the rule system.

CHAPTER VII – FINAL PROVISIONS

Article 15. Specific regulation of the Secretariat of Prizes and Betting of the Ministry of Finance will regulate the sanctions applicable to the operating agent in case of non-compliance with the provisions of this Ordinance.

Article 16. The technical requirements of live game studios and online games to be observed by the certifying entities referred to in MF/SPA Ordinance No. 300, of 2024, will be defined in a specific regulation.

Article 17. This Ordinance enters into force on the date of its publication.

REGIS ANDERSON DUDENA

****

ANNEX I – THE BETTING SYSTEM

General Requirements

1. The betting system must have an internal clock that reflects the date and time synchronized with Brasilia time - UTC-3, and provides the following information:

a) timestamping on all transactions and events;

b) timestamping of significant events; and

c) Reference clock for reports.

2. The betting system shall ensure that the time and dates between all its components, including sports betting and online gaming platforms, are synchronized.

3. The betting system shall control behaviors related to any requirement defined by the Secretariat of Prizes and Betting of the Ministry of Finance through an application or software, called a control program.

4. The betting system shall be able to verify that all critical components of the control program are authentic copies of the components approved and installed in the system, at least once every 24 hours and on demand.

5. The authentication mechanism of the control program shall:

a) use a hashing algorithm that produces a digest of the message of at least 128 bits;

b) include all critical components of the control program that may affect fixed-odds betting operations, including but not limited to executable files, libraries, betting or system settings, operating system files, components that control the

necessary system reporting, and database elements that affect system operations; and

c) indicate authentication failure if any critical component of the control program is considered invalid.

6. Each critical component of the control program shall allow for independent third-party verification, which shall operate independently of any security process or software within the system, whose integrity verification method shall be approved by the authorized certification body, prior to system approval.

7. The betting system shall be capable of performing a normal shutdown and shall only allow automatic resumption after performing at least the following procedures:

a) successful completion of the program restart routines, including self-tests;

b) authentication of all critical components of the control program, according to item 5; and

c) re-establishment and authentication of communication with all components necessary for the operation of the system.

8. The betting system shall be able to suspend, on demand:

a) all betting activities;

b) individual events;

c) individual markets;

d) individual betting devices, if any;

e) individual bettors' accounts; and

f) individual game themes, pay tables, or versions, such as desktop, mobile, tablet, and the like.

The account management of bettors

Account Registration

9. The betting system, through the bettor account management platform, must collect the bettor's information before the registration is made.

10. At the stage of registering the bettor's account, at least the following requirements must be met:

a) only bettors over the age of eighteen can register; Anyone who provides a date of birth that indicates they are a minor will be denied an account registration request;

b) any person who provides information other than their official documents shall be denied account registration;

c) identity verification must perform facial recognition and be carried out before a bettor has a registered account;

d) The Bettor's account can only be activated when:

I. age and identity verification, including CPF validity and facial recognition, is successfully completed;

II. verification that the bettor is not on any exclusion list or prohibited from establishing or maintaining an account is carried out;

III. the bettor has agreed to the privacy policies and the terms and conditions for placing bets;

IV. the bettor is aware of the prohibition of third-party access to his account;

V. the bettor has authorized the monitoring and recording of their data by the operating agent and by the Secretariat of Prizes and Betting of the Ministry of Finance; and

VI. the registration of the bettor's account is complete;

e) a bettor may only have a single active account at a time in the betting system of each brand authorized by the Secretariat of Prizes and Betting of the Ministry of Finance; and

f) The system must allow the updating of passwords or other authentication credentials, registration information and bank accounts used for financial transactions of each bettor, subject to facial recognition.

Access to the betting system

11. The betting system must authenticate the entry of any bettor registered in the system by means of a username and password or by means of biometrics. If the system does not recognize the username and/or password when entered, an explanatory message must be displayed to the bettor, asking him to re-enter the information.

12. In cases where the bettor forgets his/her username and/or password, the system must offer a multi-factor authentication process for the recovery or reset of the username and/or password, one of the factors being facial recognition.

13. If any suspicious activity is detected, such as multiple unsuccessful access attempts, the betting system shall block the respective account. In this case, in order for the account to be unlocked, a multi-factor authentication process must be carried out, one of the factors being facial recognition.

Bettor's inactivity

14. The betting system shall require a new authentication process from the bettor after a period of 30 minutes of inactivity on a device, and no bets or financial transactions will be allowed until the bettor is re-authenticated.

15. The betting system may offer, as a form of new authentication on the same device, access by biometrics, which must be tested by the certifying entity authorized by the Secretariat of Prizes and Bets of the Ministry of Finance.

16. The betting system shall require the bettor to perform multi-factor authentication:

a) at least once every 7 days; or

b) on first access after a period of inactivity of more than 7 days.

Limits and exclusions

17. The betting system shall correctly implement any limitations and exclusions established by the bettor, the operating agent and the Secretariat of Prizes and Betting of the Ministry of Finance.

18. The betting system shall not allow the bettor to impose limits that are less restrictive than those established by the operating agent and by the Secretariat of Prizes and Betting of the Ministry of Finance.

19. The established limitations shall not be affected by other internal status events.

Bettor's financial management

20. The betting system must provide confirmation or denial of all transactions carried out by the bettor.

21. The betting system must ensure that all contributions and withdrawals of financial resources by bettors are carried out exclusively by means of electronic transfer between the bettor's registered bank account and the transactional account of the operating agent, both maintained in institutions authorized to operate by the Central Bank of Brazil, pursuant to article 22 of Law No. 14,790, of 2023.

22. The betting system must ensure that the amounts contributed to the graphic account by the bettor are only available for placing bets after confirmation of the settlement of the operation by the institution maintaining the transactional account, being kept in a specific record for auditing.

23. The betting system will not allow financial transactions to be carried out on the bettor's graphic account that exceed the limits established by the bettor, the operating agent or the Secretariat of Prizes and Bets of the Ministry of Finance.

24. The betting system will not allow transfers of funds between bettors' accounts.

Account Statement

25. The betting system shall provide a statement of the last 36 months of the movements of the bettor's graphical account and a log file with the transactions made when required. The statement and log file shall include sufficient information to enable the bettor to reconcile the information provided by the operating agent with his or her bank statements, and shall include, as a minimum, the following details of the financial transactions, time-stamped and with a unique identifier of the transaction:

a) contributions to the bettor's graphic account;

b) withdrawals from the bettor's graphical account;

c) receipt of betting winnings;

d) payment of income tax on prizes;

e) manual adjustments or modifications to the bettor's graphical account, e.g. refund;

f) credits added to or removed from the bettor's graphical account related to betting;
g) means of contribution and withdrawal: electronic transfer, PIX, debit card, prepaid card and book transfer;
h) identification of the user or the betting device that processed the transaction;
i) total amount of fees paid in the transaction, if any;
j) total account balance before and after transactions; and
k) Any other transactions made in the Bettor's graphical account.

From Loyalty Programs

26. The betting system must register all transactions involving loyalty programs eventually offered to the bettor, considering the prohibitions imposed by article 29 of Law No. 14,790, of 2023, and observing the specific regulations of the Secretariat of Prizes and Bets of the Ministry of Finance.

Geolocation requirements

Location Fraud Prevention

27. The betting system shall detect the use of programs that have the ability to circumvent the detection of the bettor's location, such as remote desktop software, rootkits, virtualization and any other programs, and block the attempt to cheat the location data before the completion of each bet.

28. The betting system shall examine and log the IP address on each remote betting device connection to a network to ensure that a known Virtual Private Network (VPN) or proxy service is not in use.

29. The betting system shall detect and block devices that indicate tampering in system-level, such as rooting, jailbreaking, and the like.

30. The betting system shall identify and stop any Man-In-The-Middle attacks or similar hacking techniques and prevent code manipulation.

31. The betting system shall monitor and prevent bets placed by a single bettor's account from geographically incompatible locations, such as identifying locations in which bets were placed that would be impossible to place by moving within a short period of time.

Location detection for internet betting

32. The betting system shall have means or systems of geolocation detection that dynamically determine and monitor the location of a bettor attempting to place a bet, and that block unauthorized attempts.

33. Each bettor must undergo a location check prior to placing the first bet after accessing the betting system on a device. Subsequent checks on this device should occur every 30 minutes.

34. A geolocation method should be used to provide the bettor's physical location and associated trust radius. The certifying entity authorized by the Secretariat of Prizes and Betting of the Ministry of Finance will validate the geolocation method used.

35. Accurate sources of data should be used by the geolocation method to confirm the bettor's location.

Data Maintenance

36. The betting system shall maintain and back up all recorded data for a minimum period of 5 years.

37. The betting system shall be able to export the data for data analysis and auditing purposes in XML, XLS and CSV format at least.

38. The betting system shall keep a record, in addition to the information contained in item 25 of this Annex of the following information:

a) Sports betting:

I. unique identification number of the bet;

II. date and time at which the bet was placed;

III. identification of the IP address of the device used to place the bet;

IV. State of the Federation in which the bet was placed;

V. status of the bet: ongoing, non-winning, winning, suspended or cancelled;

VI. reason for suspension or cancellation of the bet;

VII. total amount of prize receipt and prize status: payable, paid or time-barred;

VIII. winning the bet; and

IX. Withholding Income Tax.

b) betting markets and sporting events that have been the subject of bets:

I. date and time of the start and end of the betting period;

II. date and time of the start and end of the event;

III. date and time when the results were confirmed;

IV. date and time when the winning bet was paid to the bettor;

V. number of bets and bettors;

VI. total amount of bets placed;

VII. identification of the bettor, amount and date of financial contributions;

VIII. identification of the event of the sports modality;

IX. status of the event: postponed, canceled, suspended, delayed, in progress, finished or not started;

X. fixed odds of the market which is the subject of the bet;

XI. type of market bet;
XII. total amount of prizes paid to bettors;
XIII. identification of each winning bettor;
XIV. total amount of contributions;
XV. total value of suspended and cancelled bets;
XVI. event and market identifiers;

c) Online Gambling:

I. identifier of each online gaming session;
II. IP address used to place the bet;
III. date and time of the start and end of the online gaming session;
IV. session status: awarded, non-awarded, suspended, canceled;
V. amount of bets;
VI. Identification of the bet in the online game;
VII. fixed odds of the bet;
VIII. bet amount;
IX. total amount wagered;
X. bettor's winnings;
XI. type of online play;
XII. name of the online game; and
XIII. online game certification number;

d) From each Betting Account:

I. the bettor's unique identifier;
II. date and method of identity verification, including, where applicable, a description of the identification document provided by the bettor to confirm his/her identity and the respective expiration date;
III. encrypted data of the bettor, including name, nationality, date of birth and CPF or passport, in the case of a foreign bettor;
IV. date and time of account creation;
V. date of the bettor's acceptance in relation to the terms and conditions and the operator's privacy policy;
VI. bettor's status: active, canceled, suspended, self-excluded, pending verification, judicially excluded, with registration pending annual update and validation, other;
VII. date and time of the start and end of the bettor's session;
VIII. reason for the termination of the bettor's session: inactivity, voluntary closure, termination by the operator or other reason;
IX. date and time of changes in the bettor's status;
X. established pause period;
XI. date and time of the establishment of the break period;
XII. exclusion period established;
XIII. date and time of the establishment of the exclusion period;
XIV. period of judicial exclusion determined;
XV. date and time of the determination of the period of judicial exclusion;
XVI. established limits on contributions, expenses, time and losses;

e) the operator:

I. balance of the bettors' wallets held by the operator;

II. balance of the operator's transactional accounts;

III. IRPF withheld and collected;

IV. details of legal destinations, as established in paragraph 1-A of Article 30 of Law No. 13,756, of 2018;

V. Total amount of Gross Gaming Revenue - GGR.

39. Information on the means used to place the bet shall be kept and stored in the betting system at:

a) mobile devices and computers; and

b) physical points of sale, with the identification of the terminal where the bet was placed.

40. The betting system shall maintain and store information on various events, including:

a) unsuccessful login attempts;

b) program errors and authentication incompatibilities;

c) significant periods of unavailability of any critical component of the system;

d) large winnings, individual and aggregate in a period, that exceed the amount defined in specific regulations of the Secretariat of Prizes and Bets of the Ministry of Finance, including betting registration information;

e) large bets, single and aggregated in a period, that exceed the amount defined in specific regulations of the Secretariat of Prizes and Bets of the Ministry of Finance, including betting registration information;

f) lack of responsiveness, system overrides and corrections;

g) changes to active data files that occur outside the normal execution of the program and operating system;

h) changes made to the download data library, including adding, altering, or deleting software, where supported;

i) changes to the operating system, database, network, and application policies and parameters;

j) date and time changes on the main server;

k) changes in the criteria previously established for an event or market, not including changes in the fixed shares of active markets;

l) changes in the results of an event or market;

m) Gambler Account Management:

I. adjustments to the account balance;

II. changes made to the bettor's data and confidential information recorded in the account;

III. account deactivation;

IV. large financial transactions, individual and aggregated in a period, that exceed the amount defined in a specific regulation of the Secretariat of Prizes and Betting of the Ministry of Finance, including information about the transaction;

n) irrecoverable loss of confidential information;

o) any other activity that requires user intervention and occurs outside the normal scope of operation of the system; and

p) other significant or unusual events.

41. The betting system shall maintain and store information about each employee or agent account of the operating agent, including:

a) name and position or rank;

b) functional identification;

c) complete list and description of the functions that each group or user account can perform;

d) the date and time the account was created;

e) date and time of last access;

f) date and time of the last password change; and

g) date and time when the account was disabled or deactivated.

From information to reporting

42. The betting system shall provide information on demand from the Secretariat of Prizes and Bets of the Ministry of Finance, in addition to the daily and monthly transmission of standardized information about bettors, the aggregated data of the operating agent, bets and bettors' wallets, as established in the data model contained in the SIGAP Manual.

****

ANNEX II – SPORTS BETTING PLATFORM

General requirements

1. The sports betting platform is part of the betting system and must observe the same communication, security, and other technical controls of the system.

From sports betting software

2. The betting software is used to place sports bets on real sports-themed events through the sports betting platform, integrated with the betting system.

3. The betting software, including its version, must be identified by the sports betting platform.

Software Validation

4. The betting software installed on the betting device shall be able to authenticate that all critical components contained therein are valid each time the software is loaded for use and on demand. Critical components may include, but are not limited to:

a) betting rules; and

b) elements that control communications between the betting device, the sports betting platform and the betting system, or other components necessary to ensure the proper functioning of the software.

5. In the event of authentication failure, the software shall prevent betting operations and display an appropriate error message.

User Interface Requirements

6. The interface is defined as an application through which the user views and interacts with the sports betting platform. The interface must observe the following requirements:

a) The functions of all buttons, touch or click points must be clearly indicated within the button, touch or click point area or within the help menu. There should be no functionality available through buttons, touch points, or click on the interface that is not documented;

b) any resizing or overlapping of the interface must be accurately mapped to reflect the revised view and the touch or click points;

c) the instructions of the interface, as well as the information about the functions and services provided by the software, must be clearly communicated to the user and must not be misleading or inaccurate; and

d) The display of instructions and information must be adapted to the interface.

Bet Registration Printer

7. In cases where the betting device uses a printer to issue the records to the bettor, the following information must be included:

a) date and time when the bet was placed;

b) date and time scheduled for the event;

c) any choice of bettor involved in the bet;

d) total amount wagered;

e) unique identification number or barcode of the bet;

f) unique identification of the betting device that carried out the registration; and

g) Identifier of the place where the bet was placed.

Communication

8. The software used on the platform integrated into the betting system must be programmed in such a way that it can communicate, securely, only with authorized components. If communication between the platform and the betting device is lost, the software shall prevent further operations and display an appropriate error message.

Physical Betting Devices

9. Touchscreens must be accurate and support a calibration method to maintain that accuracy. Alternatively, the display hardware can support self-calibration.

Remote Betting Devices

10. A bettor may only place a bet using the balance of his graphic account, and anonymous betting transactions are not allowed.

11. The bettor can download an application or software package integrated with the sports betting platform or access it through a browser, as long as they are integrated into the betting system.

12. The sports betting platform shall not allow bettors to transfer data of any nature between themselves, as well as to perform chat functions, through the platform.

13. The sports betting platform shall not automatically change any firewall rules specified by the device to open ports blocked by a hardware or software firewall.

14. The betting software must not access any ports that are not necessary for the communication between the remote betting device and the server that connects it to the sports betting platform and the betting system.

15. The integrity of the software may not be altered by any additional non-betting functionality.

16. Betting software should not be used to store confidential information.

Compatibility Check

17. The sports betting platform shall detect any resource limitations or incompatibilities with the betting device used by the bettor that prevent the proper operation of the software. In this case, the platform should prevent betting operations and display an error message.

Software Content

18. Betting software must not contain malicious code or functionality that is considered malicious.

Cookie Policy

19. Bettors must be informed of the use of cookies in the installation of the betting software or when accessing through internet browsers to place bets. Where cookies are required for betting, bets cannot take place if the cookie policy is not accepted by the bettor. All cookies used must not contain malicious code.

Access to information

20. The sports betting platform must be able to display directly from the user interface or from a page accessible to the bettor:

a) betting rules and content;

b) bettor protection information;
c) terms and conditions;
d) privacy policy;
e) betting and information screens; and
f) display of results.

Betting information and display

Availability of betting rules

21. The operator shall maintain and make available on the sports betting platform updated and comprehensible betting rules, market types and events offered to bettors, in addition to the rules and hypotheses related to the cancellation and suspension of bets and events.

Dynamic Betting Information

22. The operator shall display the following information to the bettor, regardless of the placing of bets:

a) information on the events and markets available for betting; and
b) up-to-date odds and prices for the available markets.

Offering features and functionality

23. Tips, suggestions and information can be offered to the bettor through the sports betting system and platform, provided that the following requirements are observed:

a) the bettor must be aware of each available feature and function, the advantage offered, and the existing options for the selection;
b) any funds involving purchase must have their cost clearly disclosed; and
c) The availability and functionality of the features must remain stable and isonomic for all bettors.

Placing bets

24. The sports betting platform shall observe the following rules regarding the placing of a bet:

a) The method of placing a bet must be simple, with all selections identified. Where the bet involves several events, these groupings must be clearly identified;
b) the platform must allow bettors to select the market on which they wish to bet;
c) the platform must not allow bets to be placed automatically on behalf of the bettor without their prior consent;
d) the platform must allow the bettors to review and confirm the selection of bets before they are submitted;
e) the platform must identify the situations in which the bettor has placed a bet for which the odds or associated prices have been modified before the bet is placed and must display a notification to confirm the bet with the new values;

f) A clear indication must be provided to the bettor that a bet has been accepted or rejected, in whole or in part. Each bet must be acknowledged and clearly stated separately, so that there is no doubt as to which bets have been accepted;

g) the balance of the bettor's graphical account must be readily accessible;

h) the platform will not accept a bet that may cause the bettor to have a negative balance; and

i) The balance of the bettor's graphic account must be debited when the bet is accepted by the platform.

Bets after the close of the allowed period

25. The platform will not allow bets to be placed after the closing of the offers.

Proof of bet

26. After the conclusion of a bet, the bettor must have access to a voucher containing the following information:

a) date and time when the bet was placed;

b) date and time when the event is expected to occur;

c) any choice of the bettor involved in the bet;

d) total amount wagered;

e) unique identification number of the bet; and

f) identifier of the device that placed the bet.

Demo mode

27. If the operating agent chooses to provide a free demo mode on the sports betting platform, in which a bettor is allowed to simulate placing bets without paying, the platform must replicate exactly the same behavior as the paid version, and the bettor is prohibited from misleading the bettor about the odds and odds available in that version.

<u>The Results</u>

Displaying the results

28. The sports betting platform shall:

a) provide the results of a bettor's bets on any decided market as soon as the results are confirmed; and

b) make available any change in the outcome of the bets.

****

ANNEX III – ONLINE GAMBLING PLATFORM

General Requirements

1. The online gaming platform is part of the betting system and must comply with the same technical requirements applicable to the system.

2. Operating agents may offer on the online gaming platform only those online games that meet the legal requirements and the specific regulation published by the Secretariat of Prizes and Betting of the Ministry of Finance.

Online gambling software

3. The gaming software is used to allow the bettor to place bets through the online gaming platform.

4. The gaming software, including its version, must be identified by the online gaming platform.

Software Validation

5. The gaming software installed on the betting device shall authenticate that all critical components contained therein are valid each time the software is loaded for use and on demand. Critical components may include, but are not limited to:

a) rules of the game;

b) payment table information; and

c) elements that control communications between the betting device, the online gaming platform and the betting system, or other components that are necessary to ensure the proper functioning of the software.

6. In case of authentication failure, the software should prevent operations and display an error message.

Communication

7. The software used in the online gaming platform must be programmed in such a way that it can communicate only with authorized components through secure communications. If communication between the platform and the device is lost, the software should prevent further bets from being placed and display an error message.

Client-Server Interactions

8. The platform shall not allow bettors to transfer data of any nature between themselves, as well as to perform chat functions, through the platform.

9. The software shall not automatically disable anti-virus or alter any firewall rules configured by the device for the purpose of opening ports that are blocked by a hardware or software firewall.

10. The software shall not access any TCP/UDP port that is not necessary for communication between the gaming device and the server.

11. If the software includes additional functionality unrelated to online games, these shall not alter the integrity of the software.

12. Software should not be used to store confidential information.

13. The software must not store any logic used to generate the result of any online game. All critical functions, including the generation of any result, must be generated by the platform and be independent of the remote gaming device used to place the bet.

Compatibility Check

14. The online gaming platform shall detect any resource limitations or incompatibilities with the betting device used by the bettor that prevent the proper operation of the software. In this case, the platform should prevent betting operations and display an error message.

Software content

15. The game software must not contain malicious code or functionality that is considered malicious.

Cookie Policy

16. Bettors must be informed of the use of cookies when installing gaming software or when accessing websites to play. Where cookies are required for online gaming, these cannot occur if the cookie policy is not accepted by the bettor. All cookies used must not contain malicious code.

Access to information

17. The online gaming platform shall display directly from the user interface or from a page accessible to the bettor:

a) the rules and content of the games;

b) information on the protection of the bettor;

c) the terms and conditions; and

d) the Privacy Policy.

Random Number Generator (RNG) requirements

18. The types of RNGs allowed are as follows:

a) Software-based RNGs: they do not use hardware devices and derive their randomness mainly from a computer- or software-based algorithm. They don't incorporate hardware randomness in any meaningful way;

b) Hardware-based RNGs: derive their randomness from small-scale physical events, such as electrical circuit feedback, electrical noise, radioactive decay, and photon spin; and

c) Mechanical RNGs: generate random game results mechanically, using the laws of physics through reels, shufflers and blowers, for example.

Source Code Requirements

19. The certifying body empowered by the Secretariat of Prizes and Betting of the Ministry of Finance shall review the source code of any and all core randomness algorithms, scaling algorithms, shuffling algorithms, and other algorithms or functions that play a critical role in generating the random result selected for use by a game.

Statistical analysis

20. The certifying entity authorized by the Secretariat of Prizes and Bets of the Ministry of Finance shall use statistical tests to evaluate the results generated by the RNG, selecting appropriate tests according to the type of RNG that is being analyzed and its use in the game.

21. The statistical tests applied by the certifying body shall be evaluated together against a 99% confidence level, and shall include one or more of the following methods:

a) total distribution or Chi-square;

b) overlap tests;

c) ticket collector tests;

d) runs tests;

e) interaction correlation tests;

f) serial correlation tests; and

g) duplication tests.

Distribution

22. Each available selection of RNG shall have the same probability of being chosen. When the game design specifies a non-uniform distribution, the result must conform to the desired distribution and observe the following requirements:

a) all scaling, mapping and shuffling algorithms used shall be unbiased and verified through a source code review, and RNG values may be discarded in this context to eliminate bias; and

b) the result shall be tested against the intended distribution using the appropriate statistical tests.

Independence

23. Knowledge of the numbers drawn in a draw shall not provide information about the numbers that may be drawn in a future draw. If the RNG selects several values within a single draw, knowing one or more values should not provide information about the other values, unless provided for in the game architecture and previously authorized by the Secretariat of Prizes and Betting of the Ministry of Finance, observing the following:

a) RNG shall not discard or modify selections based on previous selections, except as provided by the game architecture, such as in non-exchange features; and

b) The presentation of the result shall be tested for independence between draws and, if applicable, within the same draw, using appropriate statistical tests.

Available Results

24. The set of possible outcomes produced by the RNG solution shall be sufficiently large to ensure that all outcomes are available in each draw with the appropriate probability, regardless of the results previously produced, except when provided for by the game architecture and previously authorized by the Secretariat of Prizes and Betting of the Ministry of Finance.

RNG Monitoring and Strength

Strength of RNG to Determine Results

25. The RNG used to generate the results of the game on an online gaming platform must be resistant to hacker attacks using modern computational resources, and that it may have knowledge of the RNG source code.

Cryptographic RNG Attacks

26. An encrypted RNG should not be compromised by a hacker with knowledge of the source code and is resistant to the following types of attacks:

a) direct crypto-analytic attack: given a sequence of previous values generated by the RNG, it should be computationally infeasible to predict or estimate the future values of an RNG. This should be ensured through the proper use of a recognized encryption algorithm. A hardware-based RNG or a mechanical RNG may qualify as an encrypted algorithm, as long as it passes the statistical test;

b) known input attack: It should not be feasible to computationally determine or estimate the state of the RNG after the initial propagation. RNG should not be seeded solely based on a time value. Providers must ensure that games do not have the same initial seed. Propagation methods must not compromise the cryptographic strength of the RNG; and

c) state compromise extension attack: The RNG must periodically modify its state through the use of external entropy, limiting the effective duration of any successful attack attempt by a hacker.

Dynamic Results Monitoring for Hardware-Based RNGs

27. When a hardware-based RNG is used, there should be dynamic monitoring of the results by means of statistical tests. This process should disable the game when a malfunction or corruption is detected.

Mechanical RNG (physical randomness device

28. The game software will be limited to the operation of machines and the reading and writing of data of the result of the game and will not play a decisive role in its generation.

29. Devices that faithfully and mechanically create or display the result of the game generated by a computer RNG shall not be considered physical devices of randomness and shall be tested as RNGs when the faithful reproduction of the result generated from the RNG has been guaranteed.

30. Physical randomness devices will be able to incorporate RNGs into secondary functions, such as rotational speed, which will not need to be evaluated against the RNG requirements described. However, the physical randomness device should be tested as a whole.

31. Approved components of a physical randomness device shall not be replaced by non-approved components.

Data collection

32. The qualified certifying body shall collect at least 10,000 game results data using a method reasonably similar to the intended use of the device when in production.

33. The Secretariat of Prizes and Betting of the Ministry of Finance may accept as results of the tests carried out by the qualified certifying entity a smaller amount of data, which will require a statement on the statistical limitations caused by the reduced test in the certification report.

Durability

34. All mechanical parts shall be constructed of materials that prevent the degradation of any component throughout its estimated useful life.

35. The qualified certifying body may recommend a more rigorous replacement schedule than that suggested by the device manufacturer, and its periodic inspection to ensure its integrity.

Manipulation/Adulteration

36. Bettors and game attendants shall not physically manipulate or influence physical randomness devices in relation to the generation of game outcome data, unless it is designed by the game architecture, such as in the case of a game attendant pressing a button to stop a roulette wheel, or if they allow a bettor to do so.

****

ANNEX IV – GENERAL REQUIREMENTS

1. This annex contains procedures and practices related to betting operations that will be verified by the certifying entities authorized by the Secretariat of Prizes and Betting of the Ministry of Finance, under the terms of Article 8 of this Ordinance, as part of the

evaluation of the betting system, the sports betting platform and the online gaming platform.

Operation and safety of the system

System Procedures

2. The operator shall be responsible for documenting, storing and following the relevant procedures of the betting system, the sports betting platform and the online gaming platform, a procedure which shall include, at a minimum, the following requirements:

a) procedures for monitoring the critical components and data transmission of the entire system, including communication, data packets, networks, as well as the components and data transmissions of any third-party services involved, with the aim of ensuring the integrity, reliability and accessibility of the system;

b) security procedures and standards for the maintenance of all aspects of system security to ensure secure and reliable communications, including protection against hacking and adulteration;

c) procedures for defining, monitoring, documenting, investigating, reporting, responding to, and resolving security incidents and system tampering, including detected breaches and suspected or actual intrusions;

d) procedure for monitoring and adjusting resource consumption, keeping a record of system performance, including a function for compiling performance reports; and

e) procedures for investigating, documenting and resolving malfunctions, addressing:

I. determination of the cause of the malfunction;

II. analysis of relevant records, reports and surveillance records;

III. repair or replacement of the critical component;

IV. verification of the integrity of the critical component before restoring it to operation;

V. production of an incident report to the Secretariat of Prizes and Bets of the Ministry of Finance, and documenting the date, time and reason for the malfunction, together with the date and time when the system was restored; and

VI. voiding or cancelling bets and payouts if a full recovery is not possible.

Physical location of servers

3. The servers of the betting system must be securely hosted in one or more locations, meeting at least the following requirements:

a) have sufficient protection against alteration, tampering or unauthorized access;

b) be equipped with a surveillance system;

c) be protected by appropriate security perimeters and entry controls to ensure that access is restricted to authorized persons only and that any access and attempted physical access are recorded in a secure log; and

d) be equipped with controls to provide physical protection against damage caused by fires, floods, hurricanes, earthquakes, and other forms of natural or man-made disasters.

Logical Access Control

4. The betting system must be logically protected against unauthorized access by authentication credentials, such as passwords, multi-factor authentication, digital certificates, PINs, biometrics and other access methods, observing the following requirements:

a) each employee of the operator shall have his or her own individual authentication credential, the grant of which shall be controlled by means of a formal process;

b) authentication credential records should be maintained by systems that automatically record authentication changes and force changes to authentication credentials;

c) the storage of authentication credentials must be secure; If any authentication credentials are hard-coded into a system component, they must be encrypted;

d) a fallback method for authentication failure, such as forgotten passwords, must be at least as strong as the primary method;

e) lost or compromised authentication credentials and canceled user authentication credentials must be immediately disabled, secured, or destroyed;

f) The system must have multiple levels of security access to control and restrict different classes of access to the server, including viewing, changing, or deleting critical files and directories. There shall be procedures in place for assigning, reviewing, modifying, and removing access rights and privileges for each user, including:

I. permission to administer user accounts, for proper separation of duties;

II. limitation of users who have the necessary permissions to adjust the critical parameters of the system; and

III. application of appropriate authentication credential parameters, such as minimum duration and expiration intervals;

g) there should be procedures in place to identify and flag suspicious accounts where authentication credentials may have been stolen or defrauded;

h) any attempts at logical access to system applications or operating systems must be recorded in a secure log file;

i) the use of utility programs that may override application or operating system controls must be restricted and tightly controlled; and

j) When passwords are used as an authentication credential, it is recommended that they be changed at least once every 90 days, have at least 8 characters, and contain a combination of the following criteria: uppercase and lowercase letters, numeric and/or special characters.

User Authorization

5. The betting system must implement the following user authorization requirements:

a) a secure and controlled mechanism shall be employed for verification and demonstration that the system component is being operated by an authorized user on demand or on a regular basis;

b) the use of automated identification equipment to authenticate local connections and specific equipment should be documented and included in the review of access to rights and privileges;

c) any authorization information communicated by the system for identification purposes must be obtained at the time of the request and not stored in the system component; and

d) The system must allow notifications to be sent to the system administrator, and blocking the user or entering the audit trail, after a set number of unsuccessful authorization attempts.

Server Scheduling

6. The betting system and the sports betting and online gaming platforms must be sufficiently secure to prevent any programming skills initiated by the user on the server that could result in modifications to the database. However, authorized maintenance of network infrastructure or troubleshooting of applications with sufficient access rights by the network or system administrators is accepted. The server must also be protected from unauthorized execution of mobile code.

Verification Procedures

7. On-demand verification procedures shall be adopted so that the components of the critical control program of the betting system in the production environment are identical to those certified by a certifying body authorized by the Secretariat of Prizes and Betting of the Ministry of Finance, not limited to:

a) Signatures of the components of the critical control program will be collected from the production environment through the process described in item 5 of Annex I;

b) the procedure shall include one or more analytical steps to compare the current signatures of the critical control program components in the production environment with the signatures of the current approved versions;

c) The result of the procedure shall be stored in an unalterable format detailing the results of the verification for each authentication of the critical control program, and shall:

I. be recorded in a log file or system report that will be stored for a minimum period of 90 days;

II. be accessible by the Secretariat of Prizes and Betting of the Ministry of Finance in a format that allows analysis of verification records; and

III. be part of the system records that must be recovered in the event of a disaster or failure of equipment or software;

d) any failure to verify any component of the system will require a notification of authentication failure that will be communicated to the operator by means of alerts, and to the Secretary of Prizes and Betting of the Ministry of Finance, when required; and

e) There shall be a procedure in place to respond to any and all authentication failures, including determining the cause of the failure and the performance of associated fixes, as well as promoting necessary reinstallations in a timely manner.

Asset Inventory

8. All sensitive information for the storage, processing and communication of assets, including those that are part of the operating environment of the betting system and its components, must be accounted for and have an appointed owner, observing the following requirements:

a) an inventory of all assets shall be drawn up and maintained by the operator;

b) there must be a procedure for adding and removing assets;

c) a policy must be included in the acceptable use of assets associated with the system and its operating environment;

d) Each asset shall have a person designated to:

I. ensure that information and assets are appropriately classified in terms of their criticality, sensitivity and value; and

II. define and periodically review access restrictions and classifications;

e) a procedure shall be in place to ensure that the recorded accounting of assets is equivalent to current assets on an annual basis; and

f) copy protection to prevent unauthorized duplication or modification of the software may be implemented, provided that the protection method used is documented and provided to the certifying body authorized by the Secretariat of Prizes and Betting of the Ministry of Finance to ensure that the protection works as described.

Backup and Restore Procedures

Data security

9. The betting system, the sports betting platform and the online gaming platform shall provide a logical meaning to protect the bettor's and betting data, including accounting, significant event or other confidential information, against alteration, tampering or unauthorized access, subject to the following requirements:

a) appropriate methods of data manipulation should be implemented, including input validation and rejection of corrupted data;

b) the number of workstations where critical applications or associated base data can be accessed should be limited;

c) Encryption, password protection, or equivalent security should be used on files and data containing directories. Otherwise, the operator must restrict the viewing of users to the contents of such files and directories, promoting the monitoring and recording of anyone's access to them;

d) the normal operation of any data storage equipment shall not contain any options or mechanisms that could compromise the data;

e) no equipment shall have a mechanism whereby an error causes data to be automatically erased;

f) Any equipment that stores data in its memory must not allow the removal of the information unless it has first transferred information to the database or other secure components of the system;

g) the data must be stored in areas of the server that are encrypted and secure against unauthorized access;

h) the production of databases must reside on networks separate from the servers hosting any user interface;

i) data must be kept at all times, regardless of whether the server is being supplied with power; and

j) Data should be stored in such a way as to prevent data loss when parts or modules are replaced during routine maintenance.

Data Alteration

10. Alteration of any accounting, report or significant event data shall not be permitted without supervised access control. When there is a change in any data, the following information should be documented or entered into log files:

a) unique ID number for the change;

b) altered data element;

c) the value of the data element before the change;

d) the value of the data element after the change;

e) the time and date of the change; and

f) identification of the user who made the change.

Backup Frequency

11. The implementation of the backup plan should occur at least once a day.

Storage Media Backup

12. Audit log files, system databases and any other relevant bettor and betting data shall be stored using reasonable protection methods. The betting system must be designed to protect the integrity of this data when there is a failure. Redundant copies of this data should be kept on the system with open support for backups and restores, so that no failure of any part of the system can cause the loss or corruption of the data, subject to the following requirements:

a) The backup must contain a non-volatile physical media or an equivalent architectural implementation. In the event that the primary storage medium fails, the system functions and the auditing process of those functions will continue without loss of critical data;

b) in case the backup is stored on a cloud platform, another copy may also be stored on a different cloud platform;

c) If hard disk drives are used as backup media, data integrity must be ensured in the event of a disk failure. Acceptable methods include, but are not limited to, multiple hard drives in an acceptable RAID configuration or mirroring data across two or more hard drives;

d) Upon completion of the backup process, the respective media shall be immediately transferred to a location separate from the hosting location of the servers and data to which it was backed up, by temporary or permanent storage, provided that:

I. the storage location must be secured to prevent unauthorized access and provide adequate protection to prevent the permanent loss of any data; and

II. backup data files and data recovery components must be managed with at least the same level of security and system access controls; and

e) The distance between the two locations should be determined based on environmental threats and risks, power failures, and other outages, but should also consider the potential difficulty of data replication, as well as being able to access the recovery site within a reasonable time.

System failures

13. The betting system shall have sufficient redundancy and modularity so that if any single component or part of a component fails, the functions of the system and the process of auditing those functions can continue without loss of critical data. When three or more components are connected:

a) betting operations shall not be adversely affected by the resumption or recovery of any component, such as transactions that are not lost or duplicated because of the recovery of one component or another; and

b) After restarting or recovering a certain component, they must immediately synchronize the status of all transactions, data, and configurations with each other.

Accounting for master resets (main resets)

14. The operator must be able to identify and appropriately handle the situation when a master reset occurs in any component that affects betting operations.

Recovery Requirements

15. In the event of a catastrophic failure when the betting system, or any component or platform, cannot be reset in any other way, it shall be possible to restore the system from the last backup point and fully recover. The contents of this backup shall contain the following critical information, including but not limited to:

a) recorded information specified in the "Data Maintenance" section of Annex I of this Ordinance;

b) location-specific information, such as settings and security accounts;

c) encryption keys of the current system; and

d) any other system parameters, modifications, reconfigurations, additions, mergers, deletions, adjustments, and changes to parameters.

Uninterruptible Power Supply (UPS) Support

16. All components of the system must be supplied with adequate primary power. Where the server is a stand-alone application, it must have an Uninterruptible Power Supply (UPS) connected and have sufficient capacity to allow a shutdown and retention of all bettor data and bet data during a power loss. It is acceptable for the system to be able to compose a network that is supported by a UPS in which the server is included as a UPS-protected device.

Business continuity and disaster recovery plan

17. A business continuity policy and disaster recovery plan shall be adopted for the recovery of betting operations if the production environment of the betting system or any of its platforms becomes inoperable. The business continuity policy and disaster recovery plan should:

a) direct the operator in relation to the use of the method of storing the bettor's data and bets to minimize losses. If synchronous replication is used, the method for data recovery should be described or potential data loss should be documented;

b) outline the circumstances under which they will be invoked;

c) direct the operator in the establishment of a local recovery, physically separate from the production site;

d) contain recovery guides detailing the technical steps required to restore the functionality of the bet on local recovery; and

e) direct the operator in relation to the process required to summarize administrative operations of betting activities after the activation of the recovery system to a range of scenarios appropriate to the operational context of the system.

Communications

Connectivity

18. Only authorized and certified devices shall be allowed to establish communications between any component of the system. The betting system must provide a method for:

a) enroll and unenroll system components;

b) enable and disable specific system components;

c) ensure that only enabled components of the system, including betting devices, participate in betting operations; and

d) ensure that the default condition for components should be "unregistered" and "disabled".

Communication Protocol

19. Each component of the betting system shall operate as indicated by a documented security communication protocol, subject to the following requirements:

a) All protocols must use communication techniques that have appropriate error detection and recovery mechanisms designed to prevent intrusion, interference, interception, and adulteration;

b) all critical communication data for bettor or betting account management must employ encryption and authentication; and

c) Communication on the secure network shall only be possible between approved system components that have been authenticated as valid on the network. Unauthorized communications to components and access points should not be allowed.

Internet Communications and Public Networks

20. Communications between any component of the system, including betting devices, that take place on the internet and/or on a public network, must be secure. Bettor's data, sensitive information, bets, results, financial information, and bettors' transaction information must always be encrypted and protected from incomplete transmissions, misdirection, unauthorized modification of message, disclosure, duplication, or repetition.

Wireless Communications

21. Standard Wireless Local Area Network (WLAN) communications shall be secure, and possible threats and vulnerabilities shall be targeted in accordance with the operator's data security policy, and there shall be periodic inspection and verification of the integrity of the WLAN.

Network Security Management

22. Networks must be logically separated, so that there is no network traffic on a network link that cannot be served by hosts on that link. The following requirements apply:

a) Network management functions must authenticate all users on the network and encrypt all management communications;

b) failure of any single item will not result in denial of service;

c) An Intrusion Detection System/Intrusion Prevention System (IDS/IPS) shall be installed on the network, which can obey both internal and external communications, as well as detect and prevent:

I. Distributed Denial of Service (DDoS);

II. network traversal shellcode;

III. Address Resolution Protocol (ARP) forger; and

IV. other indicators of "Man-In-The-Middle" attack and cease communications immediately if detected;

d) In addition to the requirements set out in paragraph (c) of paragraph 22, an IDS/IPS installed on a WLAN shall be capable of:

I. scan the network for unauthorized access points or devices connected to any access point on the network, at least quarterly;

II. automatically disable any unauthorized device connected to the system; and

III. maintain a log file of the history of all wireless access for at least 90 days, which shall contain complete and comprehensive information about all wireless devices involved and be capable of being reconciled with all other network devices within the site or location;

e) The Network Communication Equipment (NCE) shall comply with the following requirements:

I. be constructed in such a way as to be resistant to physical damage to the hardware or corruption of the firmware/software contained therein by normal use;

II. be physically protected from unauthorized access;

III. system communications via NCE must be logically protected against unauthorized access; and

IV. if the audit log file is full, the NCE must disable all communication or offload logs to a dedicated server;

f) All network hubs, services, and connection ports must be secured to prevent unauthorized access to the network. Unused services and non-essential ports should be physically blocked and disabled by software when possible;

g) in virtualized environments, redundant server instances should not run on the same hypervisor;

h) Stateless protocols, such as User Datagram Protocol (UDP), should not be used for sensitive non-stateful transport information. Although HTTP (Hypertext Transport Protocol) is technically stateless, if it runs on the stateful Transmission Control Protocol (TCP), it is allowed;

i) all network infrastructure changes, such as network communication equipment configuration, must be recorded in a log file; and

j) Virus scanners and detection programs should be installed throughout the system, and be updated regularly to scan for new types of viruses.

Service Providers

Third-Party Communications

23. When communications with third-party service providers are implemented, such as bettor loyalty programs, financial services such as payment institutions, cloud service providers, statistical services and identity verification services, the following requirements apply:

a) the betting system and the sports betting and online gaming platforms must be able to communicate securely with the third-party service providers using encryption and strong authentication;

b) all login events involving third-party service providers must be recorded in an audit file;

c) Communication with third-party service providers must not interfere with or degrade normal functions of the betting system, subject to the following requirements:

I. data from third-party service providers should not affect bettors' communications;

II. connections to third-party service providers must not use the same network infrastructure as the bettor's connections;

III. bets must be disconnected on all network connections except the bettor's network;

IV. the system must not forward data packets from third-party service providers directly to the bettors' network and vice versa; and

V. the system must not act as an IP router between the bettor's network and third-party service providers; and

d) All financial transactions must be reconciled with the payment institutions on a daily basis.

Third-party services

24. The operator shall have policies and procedures in place to manage and monitor its adherence to the following safety requirements:

a) contracts with third-party service providers involving the access, processing, communication or management of the system and its components, or the addition of products or services to the system and its components, shall cover all relevant security requirements;

b) services, reports and records provided by third-party service providers must be monitored and reviewed annually;

c) changes in the provision of third-party service providers, including the maintenance and improvement of existing security policies, procedures and controls, should be managed, taking into account the importance of the systems and processes involved and the reassessment of risks; and

d) Third-party service providers' access rights to the system and its components shall be removed upon termination of the contract or amendment agreement or arrangement.

Technical Control

DNS Requirements

25. The following requirements apply to servers used to resolve Domain Name System (DNS) queries in association with the betting system:

a) the operator shall use a secure primary DNS server and a secure secondary DNS server that are logically and physically separate from each other;

b) the primary DNS server must be physically located in a secure data center or on a virtualized host on a suitably secure hypervisor or equivalent;

c) logical and physical access to DNS servers shall be restricted to authorized personnel;

d) Zone transfers to arbitrary hosts should not be allowed;

e) a method is required to prevent cache poisoning, such as DNSSEC - DNS Security Extension;

f) multi-factor authentication must be in place; and

g) the record lock must be in place, and therefore any request to change the DNS servers will need to be manually checked.

Cryptographic Control

26. A policy for the use of encryption controls shall be developed and implemented for the protection of information, subject to the following requirements:

a) any confidential data or information must be encrypted;

b) data that does not need to be hidden, but must be authenticated, must use some message authentication technique;

c) authentication must use a security certificate from an approved organization;

d) the encryption class used must be appropriate for the sensitivity of the data;

e) the use of encryption algorithms should be reviewed periodically to verify that they are secure;

f) Changes to encryption algorithms to correct weaknesses should be implemented as soon as possible. If such changes are not possible, the algorithm should be replaced; and

g) Encryption keys must be stored on a secure, redundant storage medium after being encrypted using a different encryption method or using a different encryption key.

Encryption Key Management

27. The management of encryption keys should follow procedures that minimally cover the following:

a) obtaining or generating encryption keys and storing them;

b) management of the expiration of encryption keys, where applicable;

c) revocation of encryption keys;

d) securely changing the configuration of the current encryption key; and

e) recovery of data encrypted with a revoked or expired encryption key for a set period after the encryption key becomes invalid.

Remote Access and Firewalls

Remote Access Security

28. Remote access is defined as any access from outside the system or system network, including access from other networks within the same location. Remote access, if used by the operator, shall:

a) be carried out by means of a secure method;

b) have an option to be disabled;

c) accept only remote connections allowed by the firewall application and system settings; and

d) be limited to functions necessary for the application to perform his/her work, and any unauthorized access is prohibited.

Remote Access Procedures and Guest Accounts

29. A procedure for controlled remote access should be established. A vendor may, with operator authorization, access the system and its associated components remotely for product and user support or upgrades and enhancements. This remote access must use specific guest accounts that will be:

a) continuously monitored by the operator;

b) disabled when not in use; and

c) restricted through logical security controls to access only those applications or databases necessary for the product, support the user, or provide updates and enhancements.

Remote Access Activity Log

30. The remote access application must maintain an automatically updated activity log file that depicts all access information, including:

a) identification of users who perform or authorize remote access;

b) Remote IP addresses, port numbers, protocols and, where possible, MAC addresses;

c) date and time when the connection was made and its duration; and

d) activity while logged in, including the specific areas accessed and changes made.

Firewalls

31. All communications, including remote access, shall pass through at least one approved application-level firewall. This includes connections to and from any non-system host used by the operator, noting the following:

a) the firewall must be located at the boundary of two different security domains;

b) a device in the same transmission domain as the system host must not have a capability that allows an alternate network path that bypasses the firewall;

c) any existing alternate network path for the purpose of redundancy shall also pass through at least one application-level firewall;

d) only applications related to the firewall can reside on it;

e) only a limited number of user accounts may be present on the firewall, such as network or system administrators;

f) the firewall must reject all connections except those that have been specifically approved;

g) the firewall must reject all connections from destinations that do not reside on the network from which the messages originate; and

h) The firewall should only allow remote access through the most up-to-date encryption protocols.

Firewall audit logs

32. The firewall application should maintain an audit log file, disable all communications, and generate an error warning if the file becomes full. The file must contain:

a) date and time of all records;

b) all firewall configuration changes;

c) all attempts to connect, whether successful or not, through the firewall; and

d) source and destination of remote IP addresses, port numbers, protocols, and, where possible, MAC addresses.

Reviewing Firewall Rules

33. Firewall rules should be periodically reviewed to verify operating conditions and the effectiveness of their security settings. This review should be performed at the entire perimeter of firewalls and internal firewalls.

<u>Change management</u>

Change Control Program Procedures

34. Change control program procedures shall be adequate to ensure that only authorized versions of programs are used in the production environment. These change controls should include:

a) a suitable software mechanism or version control for all software components and source codes;

b) Records maintained of all new installations and modifications to the system, including:

I. the date of installation or modification;

II. details of the reason or nature of the installation or change, such as new software, server repair, significant configuration modifications;

III. a description of the procedures required to put the modified or new component into service; and

IV. the identity of the user who performed the installation or modification;

c) a strategy to revert to the last implementation - rollback plan - when the installation is unsuccessful, including full backups of previous versions of the software and a test of the rollback plan prior to implementation in the production environment;

d) a policy establishing emergency change procedures;

e) change testing and migration procedures;

f) segregation of duties between developers, quality certification team, migration team and users; and

g) procedures to ensure that technical and user documentation is up-to-date after the change.

Software Development Life Cycle

35. The acquisition and development of new software shall comply with at least the following:

a) The production environment must be logically and physically separate from the development and test environment. When cloud systems are used, there can be no direct connections between the production environment and any other environment;

b) the development team should be prevented from having access to promote code changes in the production environment;

c) there must be a documented method to verify that a test software is not deployed in the production environment;

d) to prevent leakage of sensitive information, there should be a documented method to ensure that raw production data is not used in testing; and

e) All documents related to the development of the software and application must be available and retained for the duration of their lifecycle.

Bug correction

36. All bug corrections should be tested, whenever possible, in a test and development environment that is configured identically to the target production environment of the fixes. Under circumstances where error correction testing cannot be carefully conducted in time to meet timelines for the alert severity level and, if authorized, error correction

testing should be managed by risk, either by isolating or removing the untested component from the network or by applying the correction and testing after the fact.

Periodic safety tests

Technical Security Tests

37. Periodic technical security tests in the production environment shall be carried out to ensure that there are no vulnerabilities that jeopardize the security and operation of the betting system and the sports betting and online gaming platforms.

38. Testing shall consist of a security assessment method by means of a third-party attack simulation following a known methodology, and vulnerability analysis shall consist of the identification and passive quantification of the potential risk of the system.

39. Unauthorized access attempts should be made up to the highest possible level of access and should be completed with or without available authentication credentials, such as white box/black box tests. This allows evaluations to be made against hardware operating and configuration systems, including but not limited to:

a) UDP/TCP port scanning;

b) Stack fingerprinting and TCP sequence prediction to identify operating systems and services;

c) public banner grabbing;

d) web scanning using HTTP and HTTPS vulnerability scanners; and

e) scanning the router using Border Gateway Protocol (BGP) routing protocol, Border Gateway Multicast Protocol (BGMP) and Simple Network Management Protocol (SNMP).

Vulnerability Assessment

40. The purpose of vulnerability assessment is to identify vulnerabilities that could be exploited later during penetration testing by making basic queries related to the services performed on the systems in question. The evaluation shall include at least the following activities:

a) external vulnerability assessment - The targets are network devices and servers accessible by third parties, individuals or companies, through public IP, related to the system through which access to sensitive information is possible; and

b) Internal Vulnerability Assessment - Targets are internal servers related to the system through which sensitive information can be accessed. Testing of each security domain on the internal network should be performed separately.

Penetration Testing

41. The purpose of penetration testing is to exploit any weaknesses discovered during vulnerability assessment in any publicly exposed applications or systems that host applications that process, transmit, and/or store sensitive information. Penetration testing should include at least the following activities:

a) Network Layer Penetration Testing – the test mimics the actions of a real attacker who exploits weaknesses in network security, scanning systems for any weaknesses that could be used by an external attacker to disrupt the confidentiality, availability, and/or integrity of the network; and

b) Application Layer Penetration Testing - Testing uses tools to identify weaknesses in applications with authenticated and unauthenticated scans, analysis of the results to remove false positives, and manual testing to confirm the results of the tools and identify the impact of weaknesses.

42. Auditing of the Information Security Management System (ISMS) shall be performed, including all locations where confidential information is accessed, processed, transmitted, and stored. The ISMS will be reviewed against the common information security principles in relation to confidentiality, integrity and availability, such as the following sources or equivalents:

a) ISO/IEC 27001 Information Security Management System (ISMS);

b) Payment Card Industrial Data Security Standards (PCI-DSS); and

c) World Lottery Association (WLA-SCS) Security Standards.

43. An operator using a cloud service provider (CSP) to store, transmit or process sensitive information must undergo a specific audit. The CSP will be reviewed against common information security principles regarding the provision and use of cloud services, such as ISO/IEC 27017 and ISO/IEC 27018, or equivalent, noting the following:

a) if sensitive information is stored, processed, or transmitted in a cloud environment, the appropriate requirements will apply to that environment, and will typically involve validation of both CSP infrastructures and operator use of that environment;

b) the allocation of responsibility between the CSP and the Operator to manage security controls does not relieve the Operator of the responsibility to ensure that sensitive information is appropriately protected in accordance with applicable requirements; and

c) Clear policies and procedures should be agreed between the CSP and the operator for all safety requirements, and responsibilities for operation, management and reporting should be clearly defined and understood for each applicable requirement.

****

ANNEX V – GLOSSARY

Unauthorized Access - When a person gains logical or physical access without permission to a network, system, application, data, or other resource.

Remote Access - Any access from outside the system or the system's network, including any access from other networks within the same location.

System Administrator - The individuals responsible for maintaining the stable operation of the Betting System, including software infrastructure and application hardware and software.

Algorithm - A finite set of unambiguous instructions executed in a prescribed sequence to achieve a goal, especially a mathematical rule or procedure used to compute a desired outcome. Algorithms are the basis of most computer programming.

Hash Algorithm - A function that converts a string of data into a fixed-length alphanumeric string output.

Threat - Any circumstance or event with the potential to adversely affect network operations, including mission, functions, image or reputation, assets or individuals through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. In addition, it consists of the possibility of a threat source successfully exploiting a system vulnerability.

Anti-Virus - Software used to prevent, detect, and remove computer viruses, including malware, worms, and Trojan horses.

ARP, Address Resolution Protocol - The protocol used to translate IP addresses into MAC addresses to support communication over a wired or wireless local area network.

Man-In-The-Middle Attack - An attack where the attacker secretly relays and possibly alters communication between two parties who believe they are communicating directly with each other.

Authentication - The process of verifying the identity of a user, process, software package, or device, usually as a prerequisite for allowing access to resources on a system.

Message Authentication - A security measure designed to establish the authenticity of a message through an authenticator within the transmission, derived from certain predetermined elements of the message itself.

Multi-Factor Authentication - A type of authentication that uses two or more of the following elements to verify a user's identity: information known only to the user, such as a password, a pattern, or answers to challenge questions; an item owned by a user, such as an electronic token, a physical token, or an ID card; A user's biometric data, such as fingerprints, facial or voice recognition.

Backup - A copy of files and programs made for easy recovery if needed.

Banner grabbing - a technique used to obtain information from a system or network service by capturing the banner displayed in the server's response.

Biometrics - A biological identification entry, such as fingerprints or retina.

Security Certificate - Information, usually stored as a text file, that is used by the Transport Socket Layers (TSL) protocol to establish a secure connection. A security certificate contains information about who it belongs to, by whom it was issued, expiration dates, a unique serial number, or other unique identification that can be used

to verify the contents of the certificate. In order for a TSL connection to be created, both sides must have a valid Security Certificate, which is also called a Digital ID.

Barcode - A machine-readable optical representation of data. An example is a barcode found on printed betting records.

Mobile Code - Executable code that moves from one computer to another, including both legitimate code and malicious code such as computer viruses.

Key - Value used to control cryptographic operations such as decryption, encryption, generation, or verification of signatures.

Encryption Key - A cryptographic key that has been encrypted to disguise the value of the underlying plaintext.

Bettor's Account - An account held for a bettor in which information relating to bets and financial transactions is recorded in the bettor's name.

Access Control - The process of granting or denying requests to obtain and use sensitive information and related services specific to a system; and enter specific physical facilities that host critical networks or systems infrastructure.

Encryption - The conversion of data into a format, called ciphertext, that cannot be easily understood by unauthorized persons.

Bettor Data - Sensitive information about a bettor, which may include items such as their full name, date of birth, place of birth, address, phone number, or other personal information.

DDoS, Denial of Service Attack - A type of attack in which multiple compromised systems, usually infected with destructive software, are used to target a single system. The victims of a DDoS attack consist of both the end target system and all systems maliciously used and controlled by the hacker in the distributed attack.

Digest - The process in which a document, message, keyword, or other data item is condensed into a short fixed-length summary.

Betting Device - An electronic device that converts communications from the Betting System, the sports betting platform and the online gaming platform into a human-interpretable form and converts human decisions into a communication format understood by the Betting System and the platforms, allowing fixed-odds betting operations directly by the bettor. Examples of a betting device include a computer, mobile phone, and tablet.

DNS, Domain Name Service - The globally distributed Internet database that maps machine names to IP numbers and vice versa.

Domain - A group of computers and devices on a network that are administered as a unit with common rules and procedures.

IP Address - Internet Protocol Address - number assigned to each device, such as a computer, printer, smartphone connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing.

Cache Poisoning - An attack where the attacker inserts corrupted data into the Domain Name Service (DNS) cache database.

Event - Occurrence related to sports, competitions, games on which bets can be placed.

Significant Event - An occurrence that has a potential impact on the operation and that often leads to consequences and changes, such as unsuccessful access attempts, periods of system downtime, large bets, large winnings, and changes in some critical component of the system.

Firewall - A component of a computer system or network designed to block unauthorized access or traffic while at the same time allowing outside communication.

Geolocation - Identification of the real-world geographic location of a remote betting device connected to the internet.

Key Management - Activities that involve the handling of cryptographic keys and other related security parameters, such as passwords, throughout the lifecycle of keys, including their generation, storage, establishment, entry and exit, and zeroing.

Hypervisor - A hypervisor, or virtual machine monitor, is a piece of software, firmware, or hardware that creates and runs virtual machines.

HTTP - Hypertext Transfer Protocol - The underlying protocol used to define how messages are formatted and transmitted, and what actions servers and browsers should perform in response to various commands.

Data Integrity - The ownership that the data is accurate and consistent and has not been altered in an unauthorized manner in storage, during processing, and in transit.

Internet - An interconnected system of networks that connects computers around the world through the TCP/IP protocol.

IDS/IPS - Intrusion Detection System/Intrusion Prevention System - A system that inspects all incoming and outgoing network activity and identifies suspicious patterns that may indicate an attack on the network or system by someone attempting to break into or compromise a system. Used in computer security, intrusion detection refers to the process of monitoring your computer and network activities and analyzing these events to look for signs of intrusion on your system.

Printer - A peripheral Betting Device that prints betting records and betting instruments.

Sensitive Information - Information such as bettor data, betting data, validation numbers, PINs, passwords, seeds and secure keys and other data that must be treated securely.

User Interface - An application or interface program through which the user views and interacts with the Betting Software and the sports betting and online gaming platforms to communicate their actions to the Betting System.

Jailbreaking - Modification of a smartphone or other electronic device to remove restrictions imposed by the manufacturer or operator to allow the installation of unauthorized software.

Barcode Reader - A device capable of reading or interpreting a barcode. This can extend to some smartphones or other electronic devices that can run an app to scan a barcode.

MAC - Message Authentication Code - A security code that can be attached to messages or requests sent by a user for the purpose of authenticating the message.

Malware - A program that is inserted into a system, usually in a hidden manner, with the intention of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system, or to annoy or disturb the victim.

Physics Engine - Specialized software that approximates the laws of physics, including behaviors such as motion, gravity, velocity, acceleration, mass, and others, to the elements or objects of a virtual event. The physics engine is used to place the virtual event elements/objects in the context of the physical world when rendering computer graphics or video simulations.

Market - These are the different options that a player has to place their bets on a game or sporting event, such as on the winner of a football game.

Fallback method - A strategy or workaround used to deal with errors or failures of systems, processes, or interfaces, allowing the system to continue functioning properly.

Demo Mode - A game mode that allows a bettor to participate in betting without placing any financial bets, primarily for the purpose of learning or understanding the mechanics of betting.

NCE - Network Communication Equipment - One or more devices that control data communication in a system, including but not limited to cables, switches, hubs, routers, wireless access points, and telephones.

PIN - Personal Identification Number - A numeric code associated with an individual and that allows secure access to a domain, account, network, or system, for example.

Contingency Plan - Management policy and procedures designed to maintain or restore betting operations possibly at an alternate location, in the event of emergencies, system failures, or disasters.

Disaster Recovery Plan - Plan to process critical applications and prevent data loss in the event of a major hardware or software failure or destruction of facilities.

Security Policy - A document that outlines the security management framework and clearly assigns security responsibilities and lays the foundation needed to reliably measure progress and compliance.

Port - A physical entry or exit point of a module that provides access to it for physical signals, represented by logical information flows.

Critical Control Program - A software program that controls behaviors relative to any applicable technical standard and/or regulatory requirement.

Bettor loyalty program - A program that offers incentives to bettors based on the volume of play or revenue received from a bettor.

Utility Programs - Programs used to add specific functionality related to system management.

Protocol - A set of rules and conventions that specifies the exchange of information between devices, through a network or other media.

Communication and Security Protocol - A communication protocol that provides adequate protection of confidentiality, authentication, and protection of the integrity of content.

Stateless protocol - A communication scheme that treats each request as an independent transaction that is unrelated to any previous request, so that the communication consists of independent pairs of requests and responses.

Proxy - A proxy is an application that "breaks" the connection between the client and the server. The proxy accepts certain types of traffic that enter or leave a network, processes it, and forwards it. This effectively closes the direct path between the internal and external networks, making it more difficult for an attacker to obtain internal addresses and other details from the internal network.

Audit Trail - a record that shows who accessed a system and what operations the user performed during a given period.

Bet Registration - A printed ticket or electronic message confirming the acceptance of one or more bets.

Timestamp - A record of the current value of the betting system's date and time that is added to a message at the time it is created.

Betting Rules - Any written, graphic and auditory information provided to the public in connection with betting operations.

Risk - The likelihood that a threat will be successful in its attack against a network or system.

RNG - Random Number Generator - A computational or physical device, algorithm, or system designed to produce numbers in a manner indistinguishable from random selection.

Cryptographic RNG - Random Number Generator - RNG that is resistant to attack or compromise by an intelligent attacker with modern computational resources who has knowledge of the RNG's source code and/or its algorithm. Crypto RNGs cannot be feasibly "broken" to predict future values.

Rooting - Gaining access to the root code of the operating system to modify the software code on the mobile phone or other remote betting device or install software that the manufacturer would not allow to be installed.

Information Security - The process of protecting information and information systems from unauthorized access, use, disclosure, interruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

Password - A string of characters—letters, numbers, and other symbols—used to authenticate an identity or to verify access authorization.

Server - A running instance of software that is capable of accepting requests from clients and the computer running that software. Servers operate in a client-server architecture, in which "servers" are computer programs that run to fulfill the requests of other programs—"clients." In this case, the "server" would be the Event Betting System and the "clients" would be the Betting Devices.

Shellcode - A small piece of code used as a payload in security exploitation. Shellcode exploits vulnerability and allows an attacker to reduce a system's information assurance.

Betting Software - The software used to engage in betting and financial transactions with the Betting System and with the sports betting and online gaming platforms which, based on the design, is downloaded or installed on the Betting Device.

Stack fingerprinting - Systematic collection of information about a particular remote device for identification and tracking purposes.

TCP/IP - Transmission Control Protocol/Internet Protocol - It is a set of protocols that enables communication between computers and servers.

Touch Screen - A video display device that also acts as a user input device using electrical touch points on the display screen.

Virus - A self-replicating program, typically with malicious intent, that runs and spreads by modifying other programs or files.

VPN - Virtual Private Network - A private communications network built on top of a public communications network, such as the Internet, using tunneling and encryption technologies to keep the data being trafficked secure.

Vulnerability – Software, hardware, or other weaknesses in a network or system that can provide a "door" for the introduction of a threat.

Wi-Fi - The wireless LAN technology - Standard WLAN for connecting computers and electronic devices to each other and/or to the Internet.