PUBLIC PROTECTION CABINET
Kentucky Horse Racing Commission
(Emergency Amended After Comments)

809 KAR 10:003E. Technical requirements and oversight.

RELATES TO: KRS Chapter 230
STATUTORY AUTHORITY: KRS 230.260(16), 230.805, 230.811(2)
NECESSITY, FUNCTION, AND CONFORMITY: KRS 230.260(16)(a) requires the racing commission to promulgate regulations to establish standards related to sports wagering, including standards for "maintaining and auditing books and financial records, securely maintaining records of bets and wagers, integrity requirements for sports wagering and related data,. .. surveillance and monitoring systems, and other reasonable technical criteria related to conducting sports wagering." KRS 230.811(2) requires tracks and service providers to "comply with the standards established by the racing commission. .. to ensure the integrity of the system of sports wagering." KRS 230.805 establishes requirements for geolocation, technology, and servers. This administrative regulation establishes the technical standards for sports wagering technology within the state, establish testing procedures, as well the handling of changes in sports wagering technology.

Section 1. Sports Wagering Standards. A licensee shall use a sports wagering system to offer, conduct, or operate sports wagering in accordance with applicable laws and these regulations. Only an approved licensee may process, accept, offer, or solicit sports wagers.

(1) The licensee shall operate in conformity with the license conditions issued by the racing commission pursuant to KRS 230.290(3) and GLI-33 Standards.

(2) A sports wagering system shall meet the specifications established in subsection (1) of this section and these regulations. Failure to comply with the approved specifications, internal controls, or technical specifications may result in disciplinary action by the racing commission.

Section 2. Testing and Certification of Sports Wagering System. Prior to conducting sports wagering, and annually thereafter, the sports wagering system utilized by the licensee shall be submitted to a nationally recognized, independent testing laboratory approved by the racing commission for certification testing. Certification and racing commission approval shall be received prior to the use of any sports wagering system to conduct sports wagering. The licensee is responsible for all costs associated with testing and obtaining such certifications.

(1) To obtain a temporary license, a licensee may submit to the racing commission a certification report of an independent testing laboratory of a system in operation in another jurisdiction in the United States where the licensee is currently licensed or permitted. The report must certify the system to either the GLI-33 Standards or, at the discretion of the racing commission, a standard deemed to be the equivalent of the GLI-33 Standards. This alternative certification report must include a list of all critical files and associated signatures and an appendix which lists the differences of any controlled items or processes required to be certified in Kentucky which were not certified in the jurisdiction in which the report was issued. Upon review of the certification report, the racing commission will make a determination on whether to accept the certification or require additional information or documentation or testing.

(2) Unless otherwise authorized by the racing commission, the independent testing laboratory shall be provided access to the sports wagering system's controlled software source code along with the means to verify compilation of such source code. The result of the compiled source code shall be identical to that in the software submitted for evaluation.

(3) If the sports wagering system meets or exceeds the GLI-33 Standards and the commission's regulatory requirements in KAR Title 809, the independent testing laboratory approved by the racing commission shall certify the sports wagering system. Licensees are prohibited from offering sports wagering in Kentucky without such certification.

Section 3. Integration Requirements. The licensee shall be responsible for sports wagering offered by the licensee through other service providers and suppliers, and other licensees where applicable.

(1) The servers and equipment of service providers and suppliers will be considered part of the licensee's sports wagering system and shall comply with these regulations.

(2) The licensee shall guarantee that any integration with the servers and other equipment of another licensee is completed in a way that complies with these regulations.

(3) An independent testing laboratory shall conduct integration testing and certification for each critical server and other equipment with the licensee's sports wagering system prior to its deployment and as requested by the racing commission.

Section 4. Change Management Processes. The licensee shall submit change management processes to the racing commission for approval. The change management processes shall detail evaluation procedures for identifying the criticality of updates and determining which updates shall be submitted to the approved independent testing laboratory for review and certification.

(1) These change management processes shall be:

(a) Developed in accordance with the Kentucky Horse Racing Commission license conditions issued by the commission pursuant to KRS 230.290(3) and the GLI-CMP Guide;

(b) Approved by the racing commission prior to its deployment; and

(c) Available for audit by the racing commission or its designee at any time.

(2) Quarterly change reports shall be issued to the racing commission for review to ensure risk is being assessed according to the change management processes and all documentation for all changes to the critical components are complete.

(3) At least once annually, each product operating under the approved change management processes shall be fully certified to the specifications established in these regulations and other technical specifications as prescribed by the racing commission and accompanied by formal certification documentation from an independent testing laboratory. the licensee shall be allowed to seek approval for extension beyond the annual approval if hardship can be demonstrated. Granting of a hardship waiver is the sole discretion of the racing commission, upon written proof of good cause by the licensee.

Section 5. Geolocation Requirements. Mobile sports wagers shall be initiated, received, and otherwise placed in the authorized geographic boundaries within the Commonwealth of Kentucky.

(1) The geographic boundaries shall be approved by the racing commission.

(2) The licensee shall use geolocation or geofencing technology pursuant to KRS 230.805 and to monitor and block unauthorized attempts to place sports wagers when an individual or patron is physically outside the authorized geographic boundaries within the Commonwealth of Kentucky at the time the sports wager is placed.

(3) The licensee shall trigger:

(a) A geolocation check prior to the placement of the first wager after login or upon a change of IP address;

(b) Recurring periodic geolocation checks as follows:

1. For static connections, at least every twenty (20) minutes or five (5) minutes if within one (1) mile of the border; and

2. For mobile connections, at intervals to be based on a patron's proximity to the border with an assumed travel velocity of seventy (70) miles per hour or a demonstrated average velocity of a roadway/path, not to exceed twenty (20) minutes.

(4) Mechanisms shall be in place to detect software, programs, virtualization, and other technology that may obscure or falsify the patron's physical location for the purpose of placing sports wagers.

(5) Geolocation field testing shall be completed by a licensed independent test laboratory prior to an operator receiving launch authorization. The geolocation field testing shall, at a minimum, verify the following scenarios:

(a) Attempted Wagering from areas that are not authorized for wagering from multiple locations within varying distances up to the physical border;

(b) Appropriate triggering of re-geolocation frequency for both mobile and wifi connections;

(c) Geolocation check occurs immediately upon change of IP address during a user's session;

(d) Communication packet vulnerabilities including "man in the middle" attacks, replay attacks, and code manipulation are successfully defended against at least two replay attacks scenarios:

1. A network attack in which a valid positive geolocation check is captured and maliciously or fraudulently injected in place of a subsequent check, allowing a patron to wager from outside the State;

2. Potential modification or tampering of the client-side response received by the operator; and

3. Attempts to manipulate location data and remotely control devices from outside of the state.

(6) The racing commission may enter into agreements with other jurisdictions or entities to facilitate, administer, and regulate multi-jurisdictional sports wagering by licensees pursuant to KRS 230.805.

Section 6. Data Security. A licensee's data security policies shall comply with KRS 230.805. Nothing in this section shall preclude the use of internet or cloud-based hosting of such data and information or disclosure as required by Commonwealth or federal law or a court order.

Section 7. Location of Servers, Security, and Cloud Storage. A licensee shall maintain in secure locations in the Commonwealth its primary servers used to transmit information for purposes of accepting or settling of wagers on a sporting event placed by patrons in the Commonwealth.

(1) The location of all other technology and servers used by a licensee in connection with sports wagering shall be approved by the racing commission and shall be accessible by the racing commission.

(2) The racing commission may approve of the use of internet or cloud-based hosting of duplicate data or data not related to transactional wagering data upon written request of a licensee.

Section 8. Integrity and Security Assessments. Each licensee shall run integrity and security assessments that comply with GLI-33 Standards.

(1) Each licensee shall, within ninety (90) calendar days after commencing operations in Kentucky, and annually thereafter, have integrity and security assessments of the sports wagering system conducted by a third-party contractor experienced in security procedures, including, without limitation, computer security and systems security. The third-party contractor shall be selected by the licensee and shall be subject to approval of

the racing commission. Such integrity and security assessments shall include a review of the following:

(a) Network vulnerability;

(b) Application vulnerability;

(c) Application code;

(d) Wireless security;

(e) Security policy and processes;

(f) Security and privacy program management;

(g) Technology infrastructure and security controls;

(h) Security organization and governance; and

(i) Operational effectiveness.

(2) The scope of the integrity and security assessments is subject to approval of the racing commission and shall include the following:

(a) A vulnerability assessment of all digital platforms, Web sites, mobile applications, internal, external, and wireless networks with the intent of identifying vulnerabilities of all devices, the sports wagering systems, and applications transferring, storing, or processing Personally Identifiable Information or other sensitive information connected to or present on the networks;

(b) A penetration test of all digital platforms, Web sites, mobile applications, internal, external, and wireless networks to confirm if identified vulnerabilities of all devices, the sports wagering systems, and applications are susceptible to compromise;

(c) A review of the firewall rules to verify the operating condition of the firewall and the effectiveness of its security configuration and rule sets performed on all of the perimeter firewalls and the internal firewalls;

(d) A security control assessment conducted in accordance with the provisions outlined in the racing commission's regulations, including the technical security controls specified within the GLI-33 Standards, and with generally accepted professional standards approved by the racing commission.

(e) If a cloud service provider is in use, an assessment performed on the access controls, account management, logging and monitoring, and over security configurations of their cloud tenant; and

(f) An evaluation of information security services, payment services such as financial institutions and payment processors, geolocation services, and any other services which may be offered directly by the sports wagering licensee or involve the use of service providers.

(3) To qualify as a third-party contractor, the third-party contractor shall demonstrate to the commission's satisfaction, at minimum, the following qualifications:

(a) Relevant education background or in other ways provide relevant qualifications in assessing sports wagering systems;

(b) Certifications sufficient to demonstrate proficiency and expertise as a network penetration tester by recognized certification boards, either nationally or internationally; and

(c) At least three (3) years' experience performing integrity and security assessments on sports wagering systems; and

(4) The third-party contractor's full security audit report containing the overall evaluation of sports wagering in terms of each aspect of security shall be provided to the racing commission no later than thirty (30) calendar days after the assessment is conducted and shall include the following:

(a) Scope of review;

(b) Name and company affiliation, contact information, and qualifications of the individual or individuals who conducted the assessment;

(c) Date of assessment;

(d) Findings;
(e) Recommended corrective action, if applicable; and
(f) The licensee's response to the findings and recommended corrective action.

(5) It is acceptable to reuse the results of prior assessments within the past year conducted by the same third-party contractor when the testing was conducted pursuant to accepted industry standards as approved by the commission, such as International Organization for Standardization ("ISO")/International Electrotechnical Commission ("IEC") standards, the NIST Cybersecurity Framework ("CSF"), the Payment Card Industry Data Security Standards ("PCI-DSS"), or the equivalent. Such reuse shall be noted in the third-party contractor's security audit report. This reuse option does not include any critical components of a sports wagering system unique to the Commonwealth which will require fresh assessments.

(6) If the third-party contractor's security audit report recommends corrective action, the licensee shall provide the racing commission with a remediation plan and any risk mitigation plans which detail the Licensee's actions and schedule to implement the corrective action.

(a) The remediation and risk mediation plans shall be presented within a time period prescribed by the racing commission, which shall be based on at least the following factors:

1. The severity of the problem to be corrected;
2. The complexity of the problem to be corrected; and
3. The risks associated with the problem to be corrected.

(b) The commission may require suspension of operations until implementation of any critical corrective action(s).

(c) Once the corrective action has been taken, the licensee shall provide the racing commission with documentation evidencing completion.

Section 9. Quarterly Vulnerability Scans. Internal and external network vulnerability scans shall be run at least quarterly and after any significant change to the sports wagering system or network infrastructure.

(1) Testing procedures shall include protocol verifying that four (4) quarterly internal and external scans took place in the past twelve (12) months and that re-scans occurred until all "Medium Risk" (CVSS 4.0 or Higher) vulnerabilities were resolved or accepted via a formal risk acceptance program approved by the racing commission. Internal scans should be performed from an authenticated scan perspective. External scans can be performed from an uncredentialed perspective.

(2) The quarterly scans can be performed by either a qualified employee of the licensee or a qualified third-party contractor selected by the licensee and subject to approval of the racing commission.

(3) Verification of scans shall be submitted to the racing commission on a quarterly basis and within thirty (30) calendar days of running the scan. The scan verifications shall include a remediation plan and any risk mitigation plans for those vulnerabilities not able to be resolved. The commission may impose disciplinary action in the event of critical unresolved vulnerabilities or vulnerabilities that continue unabated.

JONATHAN RABINOWITZ, Chair
RAY PERRY, Secretary

APPROVED BY AGENCY: September 15, 2023
FILED WITH LRC: September 15, 2023 at 10:00 a.m.
CONTACT PERSON: Jennifer Wolsing, General Counsel, Kentucky Horse Racing Commission, 4063 Iron Works Parkway, Building B, Lexington, Kentucky 40511, phone

(859) 246-2040, fax (859) 246-2039, email jennifer.wolsing@ky.gov.