24 NCAC 06B .0408 INTEGRITY AND SECURITY ASSESSMENTS

Operators shall, within 90 Days after commencing operations in North Carolina, 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 Operator and shall be subject to approval by the Director.

(1) Integrity and security assessments shall include a review of network vulnerability, application vulnerability, website vulnerability, wireless security, security policy and processes, security and privacy program management, technology infrastructure and security controls, security organization and governance, and operational effectiveness.

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

(a) a vulnerability assessment of digital platforms, Internet websites, mobile applications, internal, external, and wireless networks with the intent of identifying vulnerabilities or potential vulnerabilities of devices, the Sports Wagering System, and applications transferring, storing, or processing Personal Information or other Sensitive Information connected to or present on the networks;

(b) a penetration test of digital platforms, Internet websites, mobile applications, and internal, external, and wireless networks to confirm if identified vulnerabilities of devices, the Sports Wagering System, 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 the perimeter firewalls and the internal firewalls;

(d) a security control assessment against the provisions adopted in these Rules, including those standards adopted in the technical security controls of the GLI-33 Standards, with generally accepted professional standards and as approved by the Director;

(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;

(f) an evaluation of information security services, payment services, geolocation services, and other services which may be offered directly by the Operator or involve the use of Service Providers or Suppliers; and

(g) other specific criteria or standards for the documented system security testing as prescribed by the Commission.

(3) To qualify as a third-party contractor, the third-party contractor shall:

(a) have relevant education background or in other ways provide relevant qualifications in assessing Sports Wagering Systems;

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

(c) three or more years' experience performing integrity and security assessments on Sports Wagering Systems; and

(d) meet other qualifications as prescribed by the Director.

(4) The full third-party contractor's security audit report containing the overall evaluation of Sports Wagering in terms of aspects of security shall be presented to the Director not later than 30 Days after the assessment is conducted and shall include:

(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, including identified or potential vulnerabilities;

(e) recommended corrective action, if applicable; and

(f) the Operator's response to the findings and recommended corrective action.

(5) It is acceptable for the audit report to leverage the results of prior assessments within the past year conducted by the same third-party contractor against standards, for example, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, the NIST Cybersecurity Framework (CSF), the Payment Card Industry Data Security Standards (PCI-DSS), or the equivalent. This leveraging shall be noted in

the third-party contractor's security audit report. This leveraging does not include critical components of a Sports Wagering System unique to the State which will require fresh assessments.

(6) If the third-party contractor's security audit report recommends corrective action, the Operator shall provide the Director with a remediation plan and risk mitigation plans which detail the Operator'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 Director, which shall be based on:

(i) the severity of the problem to be corrected;

(ii) the complexity of the problem to be corrected; and

(iii) the risks associated with the problem to be corrected.

(b) If an Operator does not implement critical corrective actions within the prescribed timeline, then it may be subject to Disciplinary Action, including Summary Suspension under Rule .0335 of Subchapter A. Before seeking to institute Disciplinary Action, the Director shall evaluate the Operator's efforts to implement available or potential mitigating controls regarding the critical items, including the timeliness of Operator's efforts, its compliance with internal controls and relevant audit report recommendations, and the scope of relevant remediation and risk plans.

(c) Once any corrective action has been completed, the Operator shall provide the Director with documentation evidencing completion.

History Note: *Authority G.S. 18C-114(a)(14);*
Previously adopted as Rule 2D-008;
Eff. January 8, 2024;
Readopted Eff. March 27, 2024.