24 NCAC 06B .0409 QUARTERLY VULNERABILITY SCANS

(a) Either a qualified employee of the Operator or a qualified third-party contractor selected by the Operator and subject to approval of the Director shall run internal and external network vulnerability scans at least quarterly and after significant changes to the Sports Wagering System or network infrastructure.

(b) Testing procedures shall verify that 4 quarterly internal and external scans took place in the past 12 months and that re-scans occurred until "High Risk" or "Critical" vulnerabilities were resolved or accepted via a formal risk acceptance program.

(1) The Operator shall submit their documented vulnerability management program that describes their risk acceptance program to the Director.

(2) Internal scans shall be performed from an authenticated scan perspective. External scans may be performed from an uncredentialed perspective.

(c) Verification of scans shall be submitted to the Director on a quarterly basis and within 30 Days of running the scan. The scan verifications shall include a remediation plan and risk mitigation plans for those vulnerabilities not able to be resolved. The severity of the vulnerabilities may be adjusted by the Operator if adhering to a formal, accepted vulnerability management plan.

(d) The Commission or Director may impose Disciplinary Action in the event of critical unresolved vulnerabilities or vulnerabilities that continue unabated that are not a result of the implementation of mitigating control.

History Note: *Authority G.S. 18C-114(a)(14);*
Previously adopted as Rule 2D-009;
Eff. January 8, 2024;
Readopted Eff. March 27, 2024.