OPERATING STANDARDS
CYBERSECURITY
EFFECTIVE DATE: NOVEMBER 1, 2023

OVERVIEW

Each Video Lottery Sales Agent (VLSA) shall submit a description of its proposed cybersecurity plan(s) for video lottery gaming activities at such time as requested by the Ohio Lottery Commission (OLC) Director or prior to commencement of video lottery gaming activities.

REFERENCE DOCUMENTS

Ohio Administrative Code 3770:2-6-03
Video Lottery Sales Agent Terms and Conditions
Operating Procedures – Minimum Internal Control Standards
Ohio Public Record Law and Security Infrastructure Exceptions ORC 149.433

STANDARDS AND COMPLIANCE

Cybersecurity plans, policies, and procedures are exempt from the public records act under section 149.433 of the Ohio Revised Code.

Cybersecurity plans, policies, and procedures must be submitted to the OLC Regulators and OLC Investigators and Security Department for approval and must address the following:

Risk Assessment

- The VLSA shall perform an initial risk assessment of its business operation and develop the cybersecurity best practices it deems appropriate.
- After performing the initial risk assessment, the VLSA shall continue to monitor and evaluate cybersecurity risks to its business operation on an ongoing basis and shall modify its cybersecurity best practices and risk assessments as it deems appropriate.
- Risk assessments and ongoing monitoring and evaluation may be performed by an affiliate of the VLSA or a third-party with expertise in the field of cybersecurity. Examples of cybersecurity best practices include, without limit, CIS Version 8, COBIT 5, ISO/IEC 27001, and NIST SP 800-53, or later versions thereof.
- The VLSA shall have until **July 1, 2024**, to fully comply with the above requirements.

Cyber-Attack Response

- A VLSA that experiences a cyber-attack to its information system resulting in a material loss of control, compromise, unauthorized disclosure of data or information, or any other similar occurrence shall:
    - Provide written notification of the cyber-attack to the OLC as soon as practicable but no later than 72 hours after becoming aware of the cyber-attack. Upon request, the VLSA shall provide the OLC with specific information regarding the cyber-attack.
    - Perform, or have a third-party perform, an investigation into the cyber-attack, prepare a report documenting the results of the investigation, notify the OLC of the completion of the report, and make the report available to OLC Regulators and OLC Investigators for review. The report must include, without limit, the root cause of the cyber-attack, the extent of the cyber-attack, and any actions taken or planned to be taken to prevent similar events that allowed the cyber-attack to occur; and

- Notify the OLC when any investigation or similar action taken by an entity external to the racino is completed and make the results of such investigation or similar action available to the OLC.

Cyber-Attack Prevention

- To mitigate the risk of a cyber-attack the VLSA shall:
  - Designate a qualified individual to be responsible for developing, implementing, overseeing, and enforcing the VLSA's cybersecurity best practices and procedures developed as required above.
  - At least annually, have its internal auditor, or other independent entity with expertise in the field of cybersecurity, perform and document observations, examinations, and inquiries to verify the VLSA is following the cybersecurity best practices and procedures developed as required above. The VLSA shall retain all documents prepared by the internal auditor. The same independent entity may be utilized to perform the procedures set forth in the paragraph below provided the procedures in this paragraph are performed by different employees.
  - At least annually, engage an independent accountant, or other independent entity with expertise in the field of cybersecurity, to perform an independent review of the VLSA's best practices and procedures developed as required above and attest in writing that those practices and procedures comply with the cybersecurity requirements outlined in this operating standard. The VLSA shall retain the written attestation, and any related documents provided therewith. The same independent entity may be utilized to perform the procedures set forth in the paragraph above provided the procedures in this paragraph are performed by different employees.

Record Retention and Reporting

- The VLSA shall retain all records required in this operating standard for a minimum of five years from the date they are created unless otherwise directed by OLC.
- The VLSA shall provide any cybersecurity related record required in this operating standard to OLC Regulators and OLC Investigators upon request.
- The VLSA's cybersecurity plan(s) shall be updated annually.

CONTACT

Questions regarding minimum internal controls, compliance reviews, and ongoing audits may be directed to: vlt@lottery.ohio.gov