PROPOSED AMENDMENTS TO
NEVADA GAMING COMMISSION REGULATIONS

Draft Dated: 10/17/2022

PURPOSE STATEMENT: To amend the Nevada Gaming Commission ("NGC") Regulations to create cybersecurity requirements for certain gaming operators; To set forth the importance of gaming operators to take necessary steps to protect their information systems from a cyber attack; To define certain terms used in the new regulation; To define which gaming operators qualify as covered entities; To require covered entities to perform an initial risk assessment and determine what best practices are necessary to mitigate the risk of a cyber attack; To require covered entities to monitor and evaluate cybersecurity risks to its business operation on an ongoing basis and modify best practices and risk assessments as necessary; To impose certain requirements should a covered entity experience certain cyber attacks; To require covered entities that are Group 1 licensees to implement certain procedures to review and verify compliance with regulation; To require covered operators to document all procedures taken to comply with the new regulation, maintain the records for five years, and provide them to the Nevada Gaming Control Board upon request; To provide that a failure to comply with the requirements of the new regulation constitutes an unsuitable method of operation; And to take such additional actions as may be necessary and proper to effectuate this stated purpose.

EFFECTIVE DATES: All changes shall become effective January 1, 2023.

EXPLANATION: Matter in *blue italics* is new language; matter in *blue italics double underlined* is new language that is to be italicized in the codified regulation; matter in *green italics underlined* is new matter added to the 9/26/2022 draft; matter in *purple italics underlined* is new matter added to the 9/27/2022 draft; matter between ~~[*red brackets italicized with a single strikethrough*]~~ is material to be omitted from the 9/26/2022 draft; and matter between ~~[*orange brackets italicized and underlined with a single strikethrough*]~~ is additional material to be omitted from the 9/27/2022 draft.

REGULATION 5

OPERATION OF GAMING ESTABLISHMENTS

5.260 Cybersecurity.

1. In accordance with the public policy of the State set forth in NRS 463.0129 and the requirements set forth in chapter 603A of NRS, it is critical that gaming operators take all appropriate steps to secure and protect their information systems from the ongoing threat of cyber attacks. Gaming operators must not only secure and protect their own records and

operations, but also the personal information of their patrons and employees as defined in NRS 603A.040.

2. Definitions. As used in this section:

(a) "Cyber attack" means any act or attempt to gain unauthorized access to an information system for purpose of disrupting, disabling, destroying, or controlling the system or destroying or gaining access to the information contained therein.

(b) "Cybersecurity" means the process of protecting an information system by preventing, detecting, and responding to cyber attacks.

(c) "Covered entity" means an entity required to comply with the requirements of this section. Each of the following qualify as a covered entity:

(1) Holder of a nonrestricted license as defined in NRS 463.0177 who deals, operates, carries on, conducts, maintains, or exposes for play any game defined in NRS 463.0152;

(2) Holder of a gaming license that allows for the operation of a race book;

(3) Holder of a gaming license that allows for the operation of a sports pool; and

(4) Holder of a gaming license that permits the operation of interactive gaming.

(d) "Information system" means a set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Elements of an information system include, without limit, hardware, software, information, data, applications, communications, and people.

(e) "Risk assessment" means the process of identifying, estimating, and prioritizing risks to organizational operations and assets resulting from the operation of an information system. Guidance for conducting a risk assessment can be found in the Framework for Improving Critical Infrastructure Cybersecurity, version 1.1 or later, published by NIST.

3. Except as otherwise provided herein, a covered entity shall perform an initial risk assessment~~[, and perform updated risk assessments as needed,]~~ of its business operation and ~~[implement]~~ develop the cybersecurity best practices it deems appropriate. After performing the initial risk assessment, the covered entity 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. The risk assessment and ongoing monitoring and evaluation required pursuant to this subsection may be performed by an affiliate of the covered entity 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. Covered entities shall have until December 31, 2023, to fully comply with this subsection.

~~[(a)The risk assessment required pursuant to this subsection may be performed by an affiliate of the covered entity or a third-party with expertise in the field of cybersecurity.~~

~~(b) A covered entity may submit a written request to the Board Chair for approval of an alternative timetable and methodology for performing the required risk assessment for multiple affiliated covered entities. The Board Chair, in his or her sole discretion, may approve or deny the request.]~~

4. A covered entity 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:

(a) ~~[Notify]~~ *Provide written notification of the cyber attack to the Board as soon as practicable but no later than 72 hours after becoming aware of the cyber attack.* ~~[The notification shall include, without limit and to the extent reasonably known at the time, a description of the nature and scope of the cyber attack, how the cyber attack was discovered, when it was discovered, whether it is ongoing, the systems affected, the impact on operations, the actions taken to contain the cyber attack, and the name of any government agencies notified, such as the FBI's Internet Crime Complaint Center. The]~~ *Upon request, the covered entity shall provide the Board with* ~~[any of the above]~~ *specific information* ~~[not available at the time of the initial notification once that information becomes available]~~ *regarding the cyber attack;*

(b) Perform, or have a third-party perform, an investigation into the cyber attack, prepare a report documenting the results of the investigation, notify the Board of the completion of the report, and make the report available to the Board for review upon request. The report must include, ~~[in addition to the information required in paragraph (a),]~~ *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*

(c) Notify the Board when any investigation or similar action taken by an entity external to the covered entity is completed and make the results of such investigation or similar action available to the Board upon request.

5. A covered entity that has been classified as a Group I licensee as defined in subsection 8 of regulation 6.010 shall:

(a) Designate a qualified individual to be responsible for developing, implementing, overseeing, and enforcing the covered entity's cybersecurity best practices and procedures developed pursuant to subsection 3.

(b) ~~*[Have]*~~ *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 of employees to verify the covered entity is following the cybersecurity best practices and procedures developed pursuant to subsection 3. A covered entity shall retain all documents prepared by the internal auditor pursuant to this paragraph in accordance with the requirements set forth in subsection 6. The same independent entity utilized under this paragraph may be utilized to perform the procedures set forth in paragraph (c) provided the procedures in this paragraph are performed by different employees.*

(c) ~~*[Engage]*~~ ~~*[Annually]*~~ *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 covered entity's best practices and procedures developed pursuant to subsection 3 and attest in writing that those practices and procedures comply with the requirements of this section. The covered entity shall retain the written attestation, and any related documents provided therewith, in accordance with the requirements set forth in subsection 6. The same independent entity utilized under this paragraph may be utilized to perform the procedures set forth in paragraph (b) provided the procedures in this paragraph are performed by different employees.*

6. A covered entity shall document in writing all procedures taken to comply with this section and the results thereof. The covered entity shall retain all records required in this section for a minimum of five years from the date they are created unless the Chair approves otherwise in writing. The covered entity shall provide any record required in this section to the Board upon request.

~~*[7. A covered entity shall attest to the Board annually as to whether it has performed the risk assessment required under subsection 3. This attestation shall be submitted on a form provided by the Board. For a covered entity that is classified as Group I licensees as defined in*~~

~~*subsection 8 of regulation 6.010, the attestation required in this subsection must be signed by the person designated by the covered entity in paragraph (a) of subsection 5.*~~ ~~]~~

~~[~~*~~8.~~*~~]~~ *7. Failure to exercise proper due diligence in compliance with this section shall constitute an unsuitable method of operation and may result in disciplinary action.*