PROPOSED AMENDMENTS TO
NEVADA GAMING COMMISSION REGULATION 5.260

Draft Dated: 11/06/2025

PURPOSE STATEMENT: To amend Nevada Gaming Commission ("NGC") Regulation 5.260(2) to add definitions for certain terms; To amend NGC Regulation 5.260(4) to modify initial notification requirements; To amend NGC Regulation 5.260(4) to require the submission of an initial incident response report; To amend NGC Regulation 5.260(4) to add a provision requiring the submission of written status reports; To amend NGC Regulation 5.260(4) to add a waiver provision for the reporting requirements set forth in the subsection; And to take such additional actions as may be necessary and proper to effectuate this stated purpose.

EFFECTIVE DATE: Upon adoption by the Nevada Gaming Commission.

EXPLANATION: Matter in *blue italics* is new language; matter between ~~[red brackets with single strikethrough]~~ is material to be omitted.

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) *"Board" has the meaning ascribed to it in NRS 463.0137.*

(b) "Chair" means the Chair of the Board.

(c) "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)]~~ *(d)* "Cybersecurity" means the process of protecting an information system by preventing, detecting, and responding to cyber attacks.

~~[(c)]~~ *(e)* "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)]~~ *(f)* "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)]~~ *(g)* "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 of its business operation and 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 fully comply with this subsection within 90 days of being licensed.

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) ~~[Provide written notification]~~ *Notify the Chair* of the cyber attack ~~[to the Board]~~ as soon as practicable but no later than ~~[72]~~ *24* hours after becoming aware of the cyber attack.

(b) Complete and submit an Initial Cyber Incident Response report within 5 calendar days after becoming aware of the cyber attack using the form provided by the Board. In lieu of this written report, a covered entity may request a meeting with the Chair to be held within the 5 calendar day period referenced herein to provide an update on the cyber attack. If such a meeting is requested, an Initial Cyber Incident

Response form shall be completed and submitted no later than 30 days from the initial reporting set forth in paragraph (a).

(c) Provide the Board with written updates regarding the cyber attack incident every 30 days from the initial reporting until the cyber attack incident is fully resolved and documented.

(d) Upon request, the covered entity shall provide the Board with specific information regarding the cyber attack;

~~[(b)]~~ *(e)* 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, 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)]~~ *(f)* 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.

➥ *The Chair, in the Chair's sole and absolute discretion, may waive or modify the reporting requirements set forth in this subsection upon the receipt of a written request from the covered entity. Any request for a waiver or modification must be submitted by the covered entity prior to any deadline related to the relevant reporting requirement. The Chair may condition or limit the waiver or modification in any manner the Chair deems appropriate. The Chair may revoke the waiver or modification at the Chair's sole and absolute discretion at any time.*

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) 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) 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. Failure to exercise proper due diligence in compliance with this section shall constitute an unsuitable method of operation and may result in disciplinary action.