24 NCAC 06A .0409 REPORTING REQUIREMENTS IN THE EVENT OF A CYBER INCIDENT

(a) The Internal Controls shall ensure that an Operator that experiences a cyber incident to its information system resulting in a material loss of control, compromise, unauthorized disclosure of data or information, or any other similar occurrence shall:

(1) provide written notification of the incident to the Director as soon as practicable but no later than 72 hours after becoming aware of the incident. Upon request, the Operator shall provide the Director with specific information regarding the incident;

(2) perform, or have a third-party perform, an investigation into the incident, prepare a report documenting the results of the investigation, notify the Director of the completion of the report, and make the report available to the Director for review upon request. The report shall include, without limit, the root cause of the incident, the extent of the incident, including detailed information about injuries to North Carolina Players, if any, planned or proposed measures to mitigate any harm to North Carolina Players, and any actions taken or planned to be taken to prevent similar events that allowed the incident to occur; and

(3) notify the Director when any investigation or similar action taken by an entity external to the Operator is completed and make the results of such investigation or similar action available to the Commission upon request.

(b) For purposes of this Rule:

(1) "cyber incident" means:

(A) any material act or material 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; or

(B) an incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing Personal Information where illegal use of the Personal Information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing Personal Information along with the confidential process or key shall constitute a cyber incident; however, good faith acquisition of Personal Information by an employee or agent of the Operator for a legitimate purpose is not a cyber incident, provided that the Personal Information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure; and

(2) "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.

(c) The requirements in this Rule are supplemental to any requirements applicable to Licensees arising under State or federal law.

History Note: *Authority G.S. 18C-114(a)(14);*
Previously adopted as Rule 1D-009;
Eff. January 8, 2024;
Readopted Eff. March 27, 2024.