Chapter 8 Information Technology

801 The Agency's Information Technology Department shall provide technical assistance to conduct thorough assessments of the Gaming Operation. The Gaming Regulatory Act addresses the Agency's information technology department regulatory functions in GRA Section § 8.5-42E.

802 Technical Component Monitoring for Slot Machine Certification

Pursuant to the provisions outlined in GRA §8.5-90, it is mandated that all gaming devices and software used within the gaming operation must adhere to Section 6A of the Compact, which states all Class III games must meet one of the following:

1. Nevada Gaming Commission and Nevada Gaming Control Board Technical Standards for Gaming Devices and Associated Equipment
2. New Jersey Administrative Code 13:69E Gaming Equipment

The Agency shall certify all gaming software and will keep detailed records of all certifications, including the date of certification, version numbers, and any applicable restrictions or conditions. The Agency will maintain and operate equipment or devices used to certify Gaming Software, including those that access databases for Independent Gaming Laboratories. The Gaming Operation shall cooperate with the Agency by providing necessary information and assistance to certify and test Gaming Devices and Gaming Software.

The Agency may conduct periodic inspections, audits, or tests to verify compliance of Gaming Devices and Gaming Software with the technical standards specified in the Compact. Non-compliance with the technical standards outlined in this regulation may result in penalties, fines, suspension, or other enforcement actions.

803 Frameworks and Standards for Information Technology, Gaming Machines, and Data Security in Casinos

All Gaming Operations within the tribe's jurisdiction must follow specific frameworks and standards for information technology, gaming machines, and data security. The Gaming Operation must establish policies and protocols that reasonably conform to the current version of the following industry-recognized frameworks, such as any of the following, or any combination of the following, subject to required revisions, if applicable:

1. NIGC 25 CFR part 543: Minimum Internal Control Standards for Class 2
2. NIGC Bulletin No. 2018-3: Guidance on the Class III Minimum Internal Control Standards
3. NHBP Gaming Commission Tribal Internal Control Standards
4. GLI-33: Standards for Event Wagering Systems
5. GLI-19: Standards for Interactive Gaming Systems
6. Michigan Gaming Control Board Regulations
7. National Institute of Standards and Technology: NIST SP 800-171 (low)
8. Payment Card Industry Data Security Standard: PCI-DSS
9. FinCEN: BSA/KYC/FIN-2016-A005 (Cybersecurity Reporting Requirement)

In instances where a Gaming Vendor is responsible for a particular control or standard, the Gaming Operation shall have the Gaming Vendor supply evidence of compliance with such standards, upon request from the Agency.

The Gaming Operation shall implement a cybersecurity program, that reasonably conforms to the current version of an industry-recognized cybersecurity framework, such as any of the following, or any combination of the following, subject to required revisions, if applicable:

1. The Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology (NIST); or
2. The Center for Internet Security Critical Security Controls for Effective Cyber Defense publication.

The Gaming Operation's policies, protocols, and/or programs shall be submitted to the Agency for approval.

804 Penetration Testing

The Gaming Operation shall conduct regular penetration testing to assess the security of its information technology systems, networks, and applications. At intervals as determined by the Executive Director, the Agency shall conduct work with a penetration testing firm or internal security team to define the scope of the testing, including the systems and applications to be tested and to ensure that all necessary preparations are in place before the testing begins. The Agency shall coordinate with the Gaming Operation's VP of IT, or their designee, to minimize disruption to normal operations during the testing.

805 Auditing of Gaming Operation IT Systems

Pursuant to this regulation, the Agency shall conduct regular information technology audits to assess the compliance of the Gaming Operation's internal controls with regard to information technology, following the protocols in the Audit chapter of the regulations. The Gaming Operation shall provide access to the Agency to all records, files, information, data and personnel, for the purposes of conducting the information technology audits required under this section.

806 Incident Reporting of Cyber Security Incidents

In accordance with industry best practices and the NIST Computer Security Incident Handling Guide (SP 800-61 Rev.2), the Gaming Operation shall establish and maintain well-defined incident reporting procedures designed to identify, classify, and respond to cybersecurity incidents based on their severity and potential impact. The incident reporting procedure shall outline the method of reporting incidents to the Agency and specify the timeframe within which incidents must be reported.

The Gaming Operation shall report all confirmed or suspected cybersecurity incidents to the Agency along with a designated incident response team promptly after their discovery, in accordance with the timeframe stipulated in the incident reporting procedure.

The response team shall implement predefined response actions, including containment, eradication, and recovery measures, to minimize the impact of the incident and restore normal operations.

Initial incident reports submitted to the Agency shall include the following information:

1. Date and Time of Initial Detection
2. Brief description of systems affected

Once the incident has been mitigated or resolved, an after action report shall be submitted to the Agency including

1. Dates and Times of Incident, including start and end dates
2. Systems affected
2. Nature of the incident
4. Vulnerabilities exploited
5. Final assessment of the incident's scope

Incident reports shall be submitted to the Agency through the approved IT email address: it@nhbpgc.org. The Gaming Operation shall ensure that incident reports are sent securely and in a manner that preserves the confidentiality and integrity of the information provided.

The Gaming Operation shall maintain accurate and comprehensive records of all incident reports, response actions, and outcomes, in accordance with the record retention period specified by the approved procedure. Detailed documentation of all cyber incident response activities, including evidence preservation and forensic analysis, shall be maintained by the organization, and provided to the Agency upon request.

807 Accepted Vulnerability Reporting

The Gaming Operation shall identity and assess Common Vulnerabilities and Exposures (CVE) of Critical or High level that pose any risk to organizational applications, data, or systems. If a Critical or High Level CVE cannot be mitigated within 30 days of finding, the Gaming Operation shall report it to the Agency through a process approved by the Agency.

Upon identification and assessment of critical or high-level vulnerabilities that are deemed an accepted risk, a comprehensive vulnerability management framework shall be implemented.

This framework should define the process for reporting accepted high-level vulnerabilities to the Agency, including the following information.

1. Detailed descriptions of identified vulnerabilities.
2. Analysis of potential impacts on the organization's applications, data, or systems.
3. Rationale for accepting the identified risk.
4. Clear recommendations for mitigating the vulnerabilities.
5. Plans for ongoing monitoring and control.

The report is to be regularly updated and reviewed as new vulnerabilities are identified or changes occur in the risk landscape and shared with the Agency.