Mille Lacs Band of Ojibwe Indians
Gaming Regulatory Authority
Office of Gaming Regulation and Compliance

July 23, 2026

NOTICE OF INTENT TO ADOPT

Pursuant to 15 MLBS § 306(b)(1), this serves as the official Notice of Intent to Adopt the following:

Changes to:
DETAILED GAMING REGULATION – 18b Information Technology

Summary of changes to DGR-18b Information Technology includes:

1. New numbering and easy to read format.
2. DGR number changed from 8 to 18b. The number will be corrected to 18 when the current DGR 18 is replaced.
3. Section 1.2 added section defining "applicable systems" when referring to Information Systems.
4. Section 1.12 added requiring a written information security policy.
5. Section 1.13 added requiring documentation of information recorded on source documents.
6. Section 1.14 added requirement for evidence of required security risk assessment.
7. Section 2.1 added covering segregation of duties for Information technology.
8. Section 6 added Incident Monitoring and Reporting.
9. Section 9 added Smart Cards / Account Access Cards – covering new technology (not yet in use or planned that we have heard, but preparing for the possibility).

Pursuant to 15 MLBSA § 306(b)(1)(i): Comments may be submitted on the proposed regulation no later than thirty (30) days from the date of the notice. The proposed regulation may be modified if supported by the data and views submitted. Comments may be submitted **no later than 8:00 a.m. on Monday, August 24, 2026,** to the Executive Director of the Office of Gaming Regulation & Compliance at **Gaming Regulatory Authority, 777 Lady Luck Drive, Hinckley, MN 55037,** or emailed to **CStaples@mlbgra.com**.

Gaming Regulatory Authority Board

7/23/26
Date

Mille Lacs Band of Ojibwe Indians

Gaming Regulatory Authority

Detailed Gaming Regulations

DGR- 18b Standards for Information Technology

Table of Contents

1. General Information Technology Standards

1.1. The Gaming Operation shall ensure that all new gaming vendor hardware and software contracts contain language requiring the vendor to adhere to the Band's internal control standards applicable to the goods and services the vendor provides.

1.2. As used in this section only, a system is any computerized system that is integral to the gaming environment. This includes, but is not limited to servers, software, hardware and peripherals for the following (collectively "Applicable Systems"):

1.2.1. Class II and Class III gaming systems.

1.2.2. Accounting systems.

1.2.3. Surveillance systems.

1.2.4. Any other systems, software or peripherals which reside on gaming networks or write to a gaming network.

1.3. Only Gaming Regulatory Authority (GRA) approved Applicable Systems and modifications to Applicable Systems may be installed.

1.4. Controls shall include the approval process for new installations or modifications of Applicable Systems, including approval/authorization by the GRA.

1.5. If an Applicable System is down for more than four (4) hours, the Gaming Operation shall promptly notify the GRA.

1.6. Documentation describing the Applicable Systems in use and the operation of those systems, such as manuals and user guides, including those for hardware, shall be maintained.

1.7. Communication procedures shall be documented for new installations or modifications, including timelines, milestones, departments impacted, etc.

1.8. Implementation procedures shall be documented for new installations or modifications, including testing, user acceptance, and "back out plans" for reversing changes, if necessary.

1.9. Records shall be maintained for all new installations and/or modifications to Applicable Systems. These records shall include, but are not limited to, the following:

1.9.1. Date of the installation or modification.

1.9.2. Nature of the installation or change such as:

a. New software.

b. Server repair.

c. Significant configuration modifications.

1.9.3. Evidence of verification that the installation or the modifications are approved by the GRA.

1.9.4. Description of procedures required to bring the new or modified program into service (conversion or input of data, installation procedures, etc.).

1.9.5. Identity of the associate(s) performing the installation and/or modification.

1.10. Testing of new and modified applications, databases, operating systems, and network changes shall be performed (by the Gaming Operation or the system manufacturer) and documented prior to implementation in the production environment. Testing shall include, but not limited to, the following (as applicable):

1.10.1. Functionality testing.

1.10.2. Reporting testing.

1.10.3. Interface testing.

1.10.4. Load and stress testing.

1.10.5. Data conversion testing.

1.10.6. User acceptance testing.

1.10.7. Post implementation testing.

1.11. The Gaming Operation shall develop a system of internal controls (SICS) for the development of in-house developed systems, including, but not limited to, the following:

1.11.1. Requests for new programs or program changes shall be reviewed by an Information Technology supervisor or above.

1.11.2. Approvals to begin work on the program shall be documented.

1.11.3. Access to implementation changes in the production environment shall be restricted and segregated from the development environment.

1.11.4. A written plan for implementation for new and modified programs shall be maintained, and include, but are not limited to, the following:

a. Date the program is to be placed into service.

b. Nature of the change.

c. Description of procedures required in order to bring the new or modified program into service (conversion or input of data, installation procedures, etc.).

d. Indication of who is to perform all such procedures.

1.11.5. Testing of new and modified in-house developed programs shall be performed and documented prior to implementation.

1.11.6. A record of the final in-house developed program or program changes shall be documented and maintained. Records shall include, but are not limited to, the following:

a. Evidence of user acceptance.

b. Date in service.

c. Programmer.

d. Reason for changes (if applicable).

1.11.7. Processes or systems shall be in place to ensure version control and accurate/complete deployment of in-house developed software updates.

1.11.8. Production changes for in-house developed systems shall be reviewed at least annually to determine that they are appropriate and approved.

1.12. The Gaming Operation shall develop an information security policy which shall be reviewed annually and communicated to relevant users. The information security policy will include, but not be limited to, the following:

1.12.1. Defined duties and responsibilities of the information security associates, including the use of super user and/or administrative accounts.

1.12.2. Procedures for user account creation/change (including user account naming standards).

1.12.3. Procedures for account suspension and termination standards (including timeliness requirement).

1.12.4. Process for reviewing access privileges at least annually.

1.12.5. Password standards (i.e., length, complexity, age, lockouts).

1.12.6. Process for how security violations are tracked, identified and resolved.

1.13. Gaming systems shall be capable of generating adequate documentation of all information recorded on the source documents and transaction details (e.g., fill/credit slips, markers, etc.).

1.13.1. Transactional source documentation shall be restricted to authorized associates.

1.13.2. Gaming system documentation shall include system exception information (e.g., appropriate system parameter information, corrections, voids, etc.).

1.14. The Gaming Operation shall provide evidence to the GRA of independent testing of IT general controls and a security risk assessment consistent with industry standards by a third party at a minimum of once every two (2) years. The scope, RFP, evaluation, vendor selection, execution and cost of each assessment will be mutually agreed to and completed by the GRA and MLCV.

2. Information Technology Segregation of Duties

2.1. The Gaming Operation shall develop SICS for the segregation of duties for the information technology functions.

2.1.1. Access granted to privileged level, shared, generic, service and/or vendor accounts shall be appropriately secured and passwords to such accounts shall be changed at least quarterly.

2.1.2. Privileged-level access shall be authorized and appropriately restricted.

2.1.3. Logging of privileged-level activity shall be enabled and monitored to detect unauthorized activity.

2.2. Information Technology associates shall be independent of the gaming areas.

2.2.1. Supervisory associates responsible for ensuring that the information technology controls are complied with shall be independent of the operation of Class II and Class III games.

2.2.2. Information Technology associates' procedures and controls must be documented and responsibilities communicated.

2.2.3. Information technology SICS shall ensure that duties are adequately segregated and monitored to detect procedural errors and to prevent the concealment of fraud.

2.3. Information Technology associates shall be precluded from unauthorized access to gaming records.

2.3.1. Gaming record access restrictions for Information Technology associates will include, but not be limited to the following:

a. Computers and terminals located in gaming areas.

b. Source documents.

c. Live data files (not test data).

2.3.2. Authorized access to gaming records shall be documented with the following:

a. The Gaming Operation supervisory associate(s) granting access shall be noted.

b. The Information Technology associate(s) granted access to restricted areas and information shall be identified.

c. A detailed description of the work performed (e.g. date, time, location, application, etc.) shall be maintained.

2.4. Information Technology associates having access to gaming systems shall not have signatory authority over financial instruments or payout forms and shall be independent of and restricted from access to the following:

2.4.1. Financial instruments.

2.4.2. Accounting, audit, and ledger entries.

2.4.3. Payout forms.

2.5. Information Technology associates shall be restricted from the following:

2.5.1. Having unauthorized access to cash or other liquid assets.

2.5.2. Initiating general or subsidiary ledger entries.

3. Physical and Logical Controls

3.1. Gaming Operation Management shall take an active role in ensuring physical and logical security measures are implemented, maintained, and adhered to by associates to prevent unauthorized access that could cause errors or compromise data or processing integrity.

3.2. The Gaming Operation shall develop SICS including, but not limited to the following:

3.2.1. Control of physical and logical environment of any systems used in conjunction with class II or class III gaming, including, but not limited to, the following:

a. Accounting.

b. VGC tickets and/or other technologically produced gaming instruments.

c. Cashless and player tracking systems.

3.2.2. Physical and logical protection of storage media and its contents, including:

a. Recovery procedures.

b. Access credential control methods.

c. Record keeping and audit processes.

3.3. The information technology environment and infrastructure shall be maintained in a secure physical location such that access is restricted to authorized people, including vendors.

3.3.1. Access devices to the systems' secured physical location, such as keys, cards, or fobs, shall be controlled by an independent department.

3.3.2. Access to the systems' secured physical location shall be restricted to authorized associates in accordance with established SICS.

3.3.3. The SICS shall include maintaining and updating a record of associated granted access privileges.

3.3.4. Network communication equipment shall be physically secured from unauthorized access.

3.4. The Gaming Operation shall develop SICS to protect all systems and to ensure that access to the following is restricted and secured:

3.4.1. System software and application programs.

3.4.2. Data associated with gaming.

3.4.3. Communications facilities, systems, and information transmissions associated with gaming systems.

3.5. Unused services and non-essential ports shall be disabled whenever possible.

3.6. Procedures shall be implemented to ensure that all activity performed on systems is restricted and secured from unauthorized access and logged.

3.7. Communications to and from systems via network communication equipment shall be logically secured from unauthorized access.

4. User Controls

4.1. Systems, including application software, shall be secured with passwords, PINs, cards, or other approved means for authorizing access where applicable.

4.2. The Gaming Operation shall develop SICS for changes to user access levels for Applicable Systems which shall include but not be limited to the following:

4.2.1. Documentation for the user access level changes.

4.2.2. Approval process for the change.

4.2.3. Process for making the user access change within the system.

4.3. For all Applicable Systems, a personnel access listing shall be maintained, which includes at a minimum the following:

4.3.1. Associate name or identification number (or equivalent).

4.3.2. Listing of functions the Associate is able to perform or equivalent means of identifying same.

4.4. Access shall be controlled as follows unless otherwise addressed in the standards in this section:

4.4.1. Each user shall have his or her own individual access credential.

4.4.2. Access credentials shall be changed at least quarterly.

4.4.3. Access credential records shall be maintained either manually or by systems that automatically record access changes and force access credential changes, including the following information for each user:

a. Associate's name.

b. Description of the access rights assigned to the associate.

c. Date the associate was given access and/or password change.

4.4.4. Only authorized associates may have access to inactive or closed accounts of other users, such as player tracking accounts and terminated associate accounts.

4.5. Generic identifications are prohibited unless access is restricted to inquiry only functions.

4.6. Lost or compromised access credentials shall be deactivated, secured or destroyed immediately.

5. Remote Access

5.1. Associates or vendors may be granted remote access for system support, provided that each access session is documented and maintained at the place of authorization. The documentation shall include the following:

5.1.1. Name of associate authorizing access.

5.1.2. Name of associate and/or vendor accessing the system.

5.1.3. Verification of the associate's and/or vendor's authorization.

5.1.4. Reason for remote access.

5.1.5. Description of work to be performed.

5.1.6. Date and time remote session began.

5.1.7. Date and time remote session ended.

5.2. All remote access shall be performed via a secure method.

6. Incident Monitoring and Reporting

6.1. The Gaming Operation shall develop SICS for information technology incident identification, management, and reporting, which shall include, but not be limited to the following:

6.1.1. Incident response and escalation protocols.

6.1.2. Incident monitoring protocols.

6.1.3. Incident notification protocols, including immediate notification to the GRA of security breaches or other significant security incidents.

6.1.4. Incident investigations.

6.1.5. Incident resolution protocols.

6.1.6. Documentation of incidents.

6.1.7. Reporting incidents.

6.2. If computer security logs are generated by the system, the logs shall be reviewed by information technology supervisory associates for evidence of the following:

6.2.1. Multiple attempts to log-on, and the system shall deny user access after five (5) attempts to log-on.

6.2.2. Unauthorized changes to live data files.

6.2.3. Any other unusual transactions.

6.3. System exception information (e.g. corrections, overrides, voids, etc.) shall be maintained.

6.4. All information technology security incidents shall be responded to within an established time period approved by the GRA and formally documented.

6.5. An information technology security/ incident report will be submitted to the GRA upon request summarizing all incidents during the requested time period and their resolution.

7. Data Backups

7.1. Controls shall include adequate backup, including, but not limited to, the following:

7.1.1. Daily data backup of critical information technology systems.

7.1.2. Data backup of critical programs or the ability to reinstall the exact programs as needed.

7.1.3. Secured storage of all backup data files and programs, or other adequate protection including off site storage.

7.1.4. Mirrored or redundant data sources.

7.2. Controls shall include recovery procedures, including, but not limited to, the following:

7.2.1. Data backup restoration.

7.2.2. Program restoration.

7.2.3. Redundant or backup hardware restoration.

7.3. Recovery procedures shall be tested on a sample basis at specified intervals at least annually. Results shall be documented and available to the GRA upon request.

7.4. Backup data files and recovery components shall be managed with at least the same level of security and access controls as the system for which they are designed to support.

8. Document Storage

8.1. Documents may be scanned or directly stored to an unalterable storage medium under the following conditions:

8.1.1. The storage medium must contain the exact duplicate of the original document.

8.1.2. All documents stored on the storage medium must be maintained with a detailed index containing the Gaming Operation department and date.

8.1.3. Upon request and adequate notice by the GRA, hardware (terminal, printer, etc.) must be made available to perform auditing procedures.

8.1.4. The storage medium must be retained for a minimum of five (5) years.

8.2. The Gaming Operation shall develop SICS that ensure the accurate reproduction of records up to and including the printing of stored documents used for auditing purposes.

8.3. Original documents shall be retained until the books and records have been audited by an independent certified public accountant.

9. Smart Cards / Account Access Cards

9.1. The Gaming Operation shall develop SICS for “smart cards” or “account access cards” if they are needed to activate the play of the machine.

9.1.1. Equipment controls shall include the following:

a. A central computer, with supporting hardware and software, to coordinate network activities, provide system interface, and store and manage a player/account database.

b. A network of contiguous player terminals with touchscreen or button-controlled video monitors connected to an electronic selection device and the central computer via a communications network.

9.1.2. Patron account maintenance controls shall include the following:

a. Functionality and recordkeeping related to deposit/withdrawal of account balances.

b. Patrons may access their accounts on the computer system by means of an account access card at the player terminal.

c. Each player terminal may be equipped with a card reader and personal identification number (PIN) pad or touch screen array for this purpose.

d. Patron password controls shall be developed, including the reset of a new PIN after a specified number of incorrect PIN entries.

e. Controls shall be developed to reset a guest's PIN in the event a customer forgets, misplaces or requests a change to their PIN.

f. All communications between the player terminal, or bank of player terminals, and the account server shall be encrypted.

9.2. For cashless systems, the Gaming Operation shall develop SICS that ensure communication between the kiosk and Applicable Systems is secure and functioning.

9.3. Smart cards, if used, cannot maintain the only source of account data.

History

History – Number change from DGR 8 to DGR 18b (number will be changed to 18 when the current 18 is replaced)

Rearranged sections

Added section 1.2 defining “applicable systems” when referring to systems covered by this DGR

Added section 1.12 requiring a written information security policy

Added section 1.13 requiring documentation of information recorded on source documents

Added section 1.14 requirement for evidence of required security risk assessment

Added section 2.1 covering segregation of duties for Information technology

Added section 6 Incident Monitoring and Reporting

Added section 9 Smart Cards / Account Access Cards – covering new technology (not yet in use or planned that we have heard, but preparing for the possibility)