Standards for Information Technology

Document No. DGR – 8 **Effective: December 17, 2013**

I. SCOPE. This document includes the Detailed Gaming Regulations for Information Technology to be regulated and played in compliance with Title 15 of the Mille Lacs Band Statutes Annotated.

II. REGULATIONS APPLICABLE TO INFORMATION TECHNOLOGY. A Gaming Enterprise shall comply with all requirements set forth in the Tribal-State Compacts, applicable Federal Regulations and Mille Lacs Band Detailed Gaming Regulations.

Section 1. The Gaming Enterprise shall implement a System of Internal Control Standards (SICS), as approved by the Gaming Regulatory Authority (GRA) Board.

Section 2. Subsequent revisions to the SICS must be provided to the GRA 30 days prior to implementation.

Section 3. The GRA reserves the right to require changes to any internal control or procedure to ensure compliance with applicable laws and regulations**.**

III. GENERAL CONTROLS FOR GAMING HARDWARE AND SOFTWARE.

Section 1. Gaming Enterprise Management shall take an active role in making sure that 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.

Section 2. Gaming Enterprise Management 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.

Section 3. Physical Security:

A. The information technology environment and infrastructure must be maintained in a secured physical location with access restricted to authorized persons, including vendors.
B. Access devices to the systems' secured physical location, such as keys, cards or fobs, must be controlled by an independent department.
C. Access to the systems' secured physical location must be restricted to associates in accordance with established policies and procedures, which must include maintaining and updating a record of agents granted access privileges.
D. Network Communication Equipment must be physically secured from unauthorized access.

Section 4. Logical Security:

A. Controls must be established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured;
    1. Systems software and application programs;
    2. Computer data; and
    3. Computer communications facilities, or the computer system, and information transmissions.
B. Unused services and non-essential ports must be disabled whenever possible.
C. All activity performed on systems is restricted, secured from unauthorized access and logged.
D. Communications to and from systems via Network Communication Equipment must be logically secured from unauthorized access.

Section 5. Access Credentials:

A. The computer systems, including application software, must be secured through the use of passwords, pins, cards or other approved means where applicable.
B. Gaming Enterprise Management associates or associates independent of the department being controlled shall assign and control access to system functions.
C. Access must be controlled as follows unless otherwise addressed in the standards in this section:
    1. Each associate must have their own individual access credential;
    2. Access credentials must be changed at least quarterly with changes documented;
    3. Either manually or by a computer system that automatically forces an access change on a quarterly basis, documentation must be maintained listing the associate's name, access rights and the date the associate was given access;
    4. Generic identifications are prohibited unless access is restricted to inquiry only functions;
    5. The system must be updated to change the status of terminated associates from active to inactive status within seventy-two (72) hours of termination;
    6. Information Technology associate usernames must be inactivated immediately upon termination;
    7. Lost or compromised access credentials must be deactivated, secured or destroyed immediately; and
    8. Only authorized associates may have access to inactive or closed accounts of other users, such as player tracking accounts and terminated user accounts.

Section 6. Data Backup and Recovery:

A. Adequate backup procedures must be in place that include, but are not limited to:
    1. Daily data backup of critical information technology systems;
    2. Data backup of critical programs or the ability to reinstall the exact programs needed;
    3. Secured off-site storage of all backup data files and programs, or other adequate protection;
    4. Mirrored or redundant data source; and
    5. Redundant or backup hardware.
B. Adequate recovery procedures must be in place that include, but are not limited to:
    1. Data backup restoration;
    2. Program restoration; and
    3. Redundant or backup hardware restoration.
C. Recovery procedures must be tested on a sample basis at least annually with documentation of results.
D. Backup data files and recovery components must be managed with at least the same level of security and access controls as the system for which they are designed to support.

IV. INDEPENDENCE OF INFORMATION TECHNOLOGY ASSOCIATES.

Section 1. Information Technology associates shall be independent of the gaming areas. Information Technology associates procedures and controls must be documented and responsibilities communicated.

Section 2. Information Technology associates shall be precluded from unauthorized access to:

A. Computers and terminals located in gaming areas;
B. Source documents; and
C. Live data files (not test data).

Section 3. Authorized access to any areas or information described in Section 2 must be documented as follows:
A. The Gaming Enterprise supervisory associate(s) granting access must be noted;
B. The Information Technology associate(s) granted access to restricted areas and information must be identified; and
C. A detailed description of the work performed (e.g. date, time, location, application, etc.) must be maintained.

Section 4. Information Technology associates shall be restricted from:
A. Having unauthorized access to cash or other liquid assets; and
B. Initiating general or subsidiary ledger entries.

Section 5. All Information Technology associates shall have signed GRA data confidentiality forms on file with OGR&C.

V. GAMING PROGRAM CHANGES.

Section 1. Only GRA approved gaming systems and modifications may be installed.

Section 2. Program changes for in-house developed systems must be documented as follows:
A. Requests for new programs or program changes must be reviewed by the Information Technology supervisor. Approvals to begin work on the program must be documented;
B. A written plan of implementation for new and modified programs must be maintained, and include, at a minimum, the date the program is to be placed into service, the nature of the change, a description of procedures required in order to bring the new or modified program into service (conversion or input of data, installation procedures, etc.), and an indication of who is to perform all such procedures;
C. Testing of new and modified programs must be performed and documented prior to implementation; and
D. A record of the final program or program changes, including evidence of user acceptance, date in service, programmer, and reason for changes, must be documented and maintained.

Section 3. New programs and program changes for purchased systems are documented as follows:
A. Documentation must be maintained that includes, at a minimum, the date the program was placed into service, the nature of the change (if applicable), a description of procedures required to the bring the new or modified program into service (conversion or input of data, installation procedures, etc.), and an indication of who performed all such procedures;
B. Testing of new and modified programs must be performed (by the licensee or the system manufacturer) and documented prior to full implementation.

Section 4. Software and hardware documentation manuals and/or user guides describing the systems and operation of each system in use must be maintained.

VI. SECURITY MONITORING AND REPORTING.

Section 1. Procedures must be implemented for responding to, monitoring, investigating, resolving, documenting and reporting security incidents associated with information technology systems.

Section 2. Security incidents must be responded to within an established time period approved by the GRA and formally documented.

Section 3. If computer security logs are generated by the system, they must be reviewed by information technology supervisory associates for evidence of:

A. Multiple attempts to log-on, or alternatively, the system shall deny user access after five (5) attempts to log-on;
B. Unauthorized changes to live data files; and
C. Any other unusual transactions.

Section 4. System exception information (e.g. corrections, overrides, voids, etc.) must be maintained.

Section 5. Sections 1-4 do not apply to personal computers.

VII. INDEPENDENT INFORMATION TECHNOLOGY REVIEW. Regular Gaming Enterprise information technology security risk assessments must be conducted by a 3rd party at a minimum 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 Corporate Commission.

VIII. REMOTE ACCESS.

Section 1. Agents may be granted remote access for system support, provided that each access session is documented and maintained at the place of authorization. The documentation must include:

A. Name of agent authorizing the access;
B. Name of agent accessing the system;
C. Verification of the agent's authorization;
D. Reason for remote access;
E. Description of work to be performed;
F. Date and time of start of end-user remote access session; and
G. Date and time of conclusion of end-user remote access session.

Section 2. Remote access must be performed via a secure method.

IX. DOCUMENT STORAGE.

Section 1. Documents may be scanned or directly stored to an unalterable storage medium under the following conditions.

A. The storage medium must contain the exact duplicate of the original document;
B. All documents stored on the storage medium must be maintained with a detailed index containing the Gaming Enterprise department and date. This index must be available to the NIGC upon request;
C. Upon request and adequate notice by the NIGC, hardware (terminal, printer, etc.) must be made available to perform auditing procedures;

D. Controls must exist to ensure the accurate reproduction of records up to and including the printing of stored documents used for auditing purposes;
E. The storage medium must be retained for a minimum of five (5) years; and
F. Original documents must be retained until the books and records have been audited by an independent certified public accountant.

History.

Changes to grammar and formatting where applicable. Change "shall" to "must" where applicable. Change "employee", "user" and "personnel" with "associate" and employees with "associates" where applicable. Change "Sections" to Parts (I. II. III.). Resume formatting after I. Delete Section 1. Implementation Deadline. Replace with "I. SCOPE. This section includes the Detailed Gaming Regulations for Information Technology to be regulated and played in compliance with Title 15 of the Mille Lacs Band Statutes Annotated." Added Part II. REGULATIONS APPLICABLE TO INFORMATION TECHNOLOGY. A Gaming Enterprise shall comply with all requirements set forth in the Tribal-State Compacts, applicable Federal Regulations and Mille Lacs Band Detailed Gaming Regulations. The Gaming Enterprise shall implement a System of Internal Control Standards (SICS), as approved by the Gaming Regulatory Authority (GRA) Board. Section 1 Subsequent revisions to the SICS must be provided to the GRA 30 days prior to implementation of revision. Section 2 The GRA reserves the right to require changes to any internal control or procedure to ensure compliance to applicable laws and regulations**.** Part III Section 2: deleted "An example of such language shall be presented to the GRA Board for its approval within ninety (90) days of Band Assembly's approval of the Initial Detailed Gaming Regulations." after *providing.* Part III Section 3: added Physical Security: The information technology environment and infrastructure must be maintained in a secured physical location with access restricted to authorized persons, including vendors.Access devices to the systems' secured physical location, such as keys, cards, or fobs, must be controlled by an independent department. Access to the systems' secured physical location must be restricted to associates in accordance with established policies and procedures, which must include maintaining and updating a record of agents granted access privileges. Network Communication Equipment must be physically secured from unauthorized access. Part III Section 3: deleted "security measures shall exist over computer, computer terminals" after *Physical* Part III Section 3(A): deleted "storage media to prevent" after *and* Part III Section 3(D): deleted "and loss of integrity of data and processing." after *access* Part III Section 4: added Logical Security: Controls must be established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured; Part III Section 4(A)(1), (2) and (3): deleted "shall be limited to authorized associates" Part III Section 4(A)(2): added "; and" after *data* Part III Section 4: deleted "Standards in paragraph (A)(i) of this section shall apply to each applicable department within the Gaming Enterprise." Part III Section 4: deleted (B)The main computers (i.e., hardware, software, and data files) for each gaming application (e.g., gaming machines, table games, etc.) shall be in a secured area with access restricted to authorized persons, including vendors. (C)Access to computer operations shall be restricted to authorized associates to reduce the risk of loss of integrity of data or processing. (D)Incompatible duties shall be adequately segregated and monitored to prevent error in general information technology procedures to go undetected or fraud to be concealed. (E) Non-information technology associates shall be precluded from having unrestricted access to the secured computer areas. Part III Section 4: added B. Unused services and non-essential ports must be disabled whenever possible. C. All activity performed on systems is restricted, secured from unauthorized access and logged. D. Communications to and from systems via Network Communication Equipment must be logically secured from unauthorized access. Part III added Section 5. Access Credentials: Part III Section 5(A): added "pins, cards" after *passwords,* Part III Section 5(C): deleted "Usernames and passwords" and replaced with "Access" before *shall P*art III Section 5(C)(1): replaced "user shall" with "associate must" after *Each* and replaced "username and password" with "access credential" after *individual* Part III Section 5(C)(2): replaced "Passwords shall" with "Access credentials must" before *be* Part III Section 5(C)(3): replaced "For" with "Either manually or by a" before *computer*; "force a password" with "forces an access" before *change;* and "systems" with "associate's name, access rights" before *and.* Part III Section 5(C)(5): replaced "is" with "must be" and removed "and" Part III Section 5(C): added "7. Lost or compromised access credentials must be deactivated, secured or destroyed immediately; and" Part III Section 5(C): added "8. Only authorized associates may have access to inactive or closed accounts of other users, such as player tracking accounts and terminated user accounts." Part III: added Section 6. Data Backup and Recovery, was formerly (I) Part III Section 6(A): deleted "and recovery"; added "but are not limited to:" after *include* Part III Section 6(A)(1): replaced "Frequent" with "Daily data"; and replaced "data files" with "critical information technology systems;" after *of* Part III Section 6(A)(3): deleted "and" after *protection;* Part III Section 6(A): added (4) and (5) 4. Mirrored or redundant data source; and 5. Redundant and/or backup hardware. Part III Section

6: added (B) Adequate recovery procedures must be in place that include but are not limited to: Data backup restoration; Program restoration; and Redundant or backup hardware restoration. Part III Section 6(C): replaced "which are" with "must be" Part III: deleted original (J) "Adequate information technology system documentation shall be maintained, including descriptions of hardware and software, operator manuals, etc." Part III Section 6: added "(D). Backup data files and recovery components must be managed with at least the same level of security and access controls as the system for which they are designed to support." Section 3 now Part IV. INDEPENDENCE OF INFORMATION TECHNOLOGY ASSOCIATES. Part IV Section 1: added "Information Technology" before *associates*; removed "(e.g., cage, pit, count rooms, etc.)"; and replaced "should" with "must" before *be.* Part IV Section 3: replaced "part (B) of this section shall" with "Section 2 must" Section 4. not Part V. GAMING PROGRAM CHANGES. Part V Section 1: added "Only GRA approved gaming systems and modifications may be installed." Part V Section 3: deleted "A copy of the software program documentation as stated in part (i) of this section shall be submitted to the GRA Board for each new program or program change; and" Part V Section 4: added "Software and hardware documentation manuals and/or user guides describing the systems and operation of each system in use must be maintained." Added Part VI. SECURITY MONITORING AND REPORTING. Section 1. Procedures must be implemented for responding to, monitoring, investigating, resolving, documenting and reporting security incidents associated with information technology systems. Section 2. Security incidents must be responded to within an established time period approved by the GRA and formally documented. Part VI Section 3(A): replaced "three" with "five (5)" Part VI Section 5: replaced "shall" with "does". Section 8. replaced by VIII. REMOTE ACCESS Part VIII Section 1: added "Agents may be granted remote access for system support, provided" before *that;* deleted "can be accessed remotely by a vendor, the following procedures shall be"; added "each access session is documented and" before *maintained*; deleted "that"; added "at the place of authorization. The documentation must" before *include*; deleted "at a minimum:" Part VIII: deleted "(i) Type of application, vendor's name and business address and version number, if applicable; (ii) The procedures used in establishing and using passwords to allow authorized vendor personnel to access the system through remote access; (iii) The associates/positions involved and procedures performed to enable the physical connection to the system when the vendor requires access to the system through remote access; and (iv) The associates/positions involved and procedures performed to ensure the physical connection is disabled when the remote access is not in use." Part VIII Section 1: deleted "In the event of remote access by a vendor, the Gaming Enterprise shall maintain an access log that includes:" Part VIII Section 1(A): replaced "associate" with "agent"; added "the" before *access* Part VIII Section 1(B): replaced "authorized programmer or manufacturer representative" with "agent accessing the system;" Part VIII Section 1(C): added "Verification of the agent's authorization;" Part VIII Section 1(D): added "remote" before *access* Part VIII Section 1(E): added "to be" before *performed*; deleted "(adequately detailed to include the old and new version of any software that was modified and details regarding any other changes made to the system)" Part VIII Section 1(F): added "and" before *time;* replaced "and duration" with "of start"; added "end-user remote" before *access*; added "session; and" Part VIII Section 1(G): added "Date and time of conclusion of end-user remote access session." Part VIII Section 2: "Remote access must be performed via a secure method." Section 9 now Part IX. DOCUMENT STORAGE

Each Gaming Enterprise shall come into compliance with changes no later than October 1, 2014. Each Gaming Enterprise may petition the GRA Board for an extension of up to six (6) months. Approval of an extension is discretionary.