



Mille Lacs Band of Ojibwe Indians
Gaming Regulatory Authority
Detailed Gaming Regulations

Standards for Information Technology

Document No. DGR - 8

Effective: November 10, 2005

Section 1. Implementation Deadline. Within ninety (90) days of the approval of these Initial Detailed Gaming Regulations by the Band Assembly pursuant to the procedures contained in Title 15 of the Mille Lacs Band Statutes Annotated, the Band's Gaming Enterprises or the Corporate Commission, at the Corporate Commission's discretion, shall:

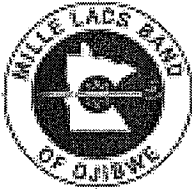
- (i) submit to the Gaming Regulatory Authority Board ("GRA Board") for its approval procedures required in these Standards for Information Technology; and
- (ii) implement the requirements of these Standards for Information Technology.

Section 2. General controls for gaming hardware and software.

- (A) Gaming Enterprise Management shall take an active role in making sure that physical and logical security measures are implemented, maintained, and adhered to by personnel to prevent unauthorized access that could cause errors or compromise data or processing integrity.
- (i) Gaming Enterprise Management shall ensure that all new gaming vendor hardware and software agreements/contracts contain language requiring the vendor to adhere to the Band's internal control standards applicable to the goods and services the vendor is providing. 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.
 - (ii) Physical security measures shall exist over computer, computer terminals, and storage media to prevent

unauthorized access and loss of integrity of data and processing.

- (iii) Access to systems software and application programs shall be limited to authorized associates.
 - (iv) Access to computer data shall be limited to authorized associates.
 - (v) Access to computer communications facilities, or the computer system, and information transmissions shall be limited to authorized associates.
 - (vi) Standards in paragraph (A)(i) of this section shall apply to each applicable department within the Gaming Enterprise.
- (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.
- (G) The computer systems, including application software, shall be secured through the use of passwords or other approved means where applicable. Gaming Enterprise Management associates or persons independent of the department being controlled shall assign and control access to system functions.
- (H) Usernames and passwords shall be controlled as follows unless otherwise addressed in the standards in this section:



Mille Lacs Band of Ojibwe Indians
Gaming Regulatory Authority
Detailed Gaming Regulations

Standards for Information Technology

Document No. DGR - 8

Effective: November 10, 2005

-
- (i) Each user shall have their own individual username and password;
 - (ii) Passwords shall be changed at least quarterly with changes documented;
 - (iii) For computer systems that automatically force a password change on a quarterly basis, documentation shall be maintained listing the systems and the date the user was given access;
 - (iv) Generic identifications are prohibited unless access is restricted to inquiry only functions;
 - (v) The system is updated to change the status of terminated associates from active to inactive status within seventy-two (72) hours of termination; and
 - (vi) Information technology associate usernames shall be inactivated immediately upon termination.
- (I) Adequate backup and recovery procedures shall be in place that include:
- (i) Frequent backup of data files;
 - (ii) Backup of all programs;
 - (iii) Secured off-site storage of all backup data files and programs, or other adequate protection; and
 - (iv) Recovery procedures, which are tested on a sample basis at least annually with documentation of results.
- (J) Adequate information technology system documentation shall be maintained, including descriptions of hardware and software, operator manuals, etc.
- Section 3. Independence of information technology associates.**
- (A) The information technology associates shall be independent of the gaming areas (e.g., cage, pit, count rooms, etc.). Information technology associates procedures and controls should be documented and responsibilities communicated.
- (B) Information technology associates shall be precluded from unauthorized access to:
- (i) Computers and terminals located in gaming areas;
 - (ii) Source documents; and
 - (iii) Live data files (not test data).
- (C) Authorized access to any areas or information described in part (B) of this section shall be documented as follows:
- (i) The Gaming Enterprise supervisory associate(s) granting access shall be noted;
 - (ii) The information technology associate(s) granted access to restricted areas and information shall be identified; and
 - (iii) A detailed description of the work performed (e.g. date, time, location, application, etc.) shall be maintained.
- (D) Information technology associates shall be restricted from:
- (i) Having unauthorized access to cash or other liquid assets; and
 - (ii) Initiating general or subsidiary ledger entries.
- (E) All information technology associates shall have signed GRA data confidentiality forms on file with OGR&C.
- Section 4. Gaming program changes.**
- Program changes for in-house developed systems shall be documented as follows:
- (i) Requests for new programs or program changes shall be reviewed by the information technology supervisor. Approvals to begin work on the program shall be documented;
 - (ii) A written plan of implementation for new and modified programs shall be maintained, and shall include, at a minimum, the date the program is to be placed into service, the nature of the change, a description of procedures



Mille Lacs Band of Ojibwe Indians
Gaming Regulatory Authority
Detailed Gaming Regulations

Standards for Information Technology

Document No. DGR - 8

Effective: November 10, 2005

- 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;
- (iii) Testing of new and modified programs shall be performed and documented prior to implementation; and
 - (iv) A record of the final program or program changes, including evidence of user acceptance, date in service, programmer, and reason for changes, shall be documented and maintained.

Section 5. Purchased software programs.

New programs and program changes for purchased systems are documented as follows:

- (i) Documentation shall 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 in order to 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;
- (ii) 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
- (iii) Testing of new and modified programs shall be performed (by the licensee or the system manufacturer) and documented prior to full implementation.

Section 6. Security logs.

- (A) If computer security logs are generated by the system, they shall be reviewed by

information technology supervisory associates for evidence of:

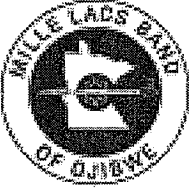
- (i) Multiple attempts to log-on, or alternatively, the system shall deny user access after three attempts to log-on;
 - (ii) Unauthorized changes to live data files; and
 - (iii) Any other unusual transactions.
- (B) System exception information (e.g. corrections, overrides, voids, etc.) shall be maintained.
 - (C) This section shall not apply to personal computers.

Section 7. Independent information technology review.

Regular Gaming Enterprise information technology security risk assessments shall 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.

Section 8. Remote access.

- (A) For each computerized Gaming Enterprise application that can be accessed remotely by a vendor, the following procedures shall be maintained that include, at a minimum:
 - (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



Mille Lacs Band of Ojibwe Indians
Gaming Regulatory Authority
Detailed Gaming Regulations

Standards for Information Technology

Document No. DGR - 8

Effective: November 10, 2005

- (iv) The associates/positions involved and procedures performed to ensure the physical connection is disabled when the remote access is not in use.
- (B) In the event of remote access by a vendor, the Gaming Enterprise shall maintain an access log that includes:
 - (i) Name of associate authorizing access;
 - (ii) Name of authorized programmer or manufacturer representative;
 - (iii) Reason for access;
 - (iv) Description of work performed (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); and
 - (v) Date, time, and duration of access.

- (vi) Original documents must be retained until the books and records have been audited by an independent certified public accountant.

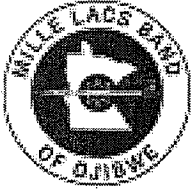
History. Approved by Band Assembly on November 10, 2005.

Changes to all applicable sections gaming operation to Gaming Enterprise; Changes to all applicable sections employee(s) and personnel to associate(s); Changes to section 2(B) deleted keno, race and sports and added table games; Changes to section 2(H) and 2(H)(i) added usernames and; Changes to section 2(H)(ii) deleted and; Addition of sections 2(H)(iv - vi), (iv) Generic identifications are prohibited unless access is restricted to inquiry only functions; (v) The system is updated to change the status of terminated associates from active to inactive status within seventy-two (72) hours of termination; and (vi) Information technology associate usernames shall be inactivated immediately upon termination; Addition of section 3(C), Authorized access to any areas or information described in part (B) of this section shall be documented as follows: (i) The Gaming Enterprise supervisory associate(s) granting access shall be noted; (ii) The information technology associate(s) granted access to restricted areas and information shall be identified; and (iii) A detailed description of the work performed (e.g. date, time, location, application, etc.) shall be maintained; Addition of section 3(E), All information technology associates shall have signed GRA data confidentiality forms on file with OGR&C; Changes to section 4, removed only citation (A); Changes to section 4(iv), removed record; Addition of section 5, Purchased software programs. New programs and program changes for purchased systems are documented as follows: (i) Documentation shall 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 in order 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; (ii) A copy of the software program

Section 9. Document storage.

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

- (i) The storage medium shall contain the exact duplicate of the original document.
- (ii) All documents stored on the storage medium shall be maintained with a detailed index containing the Gaming Enterprise department and date. This index shall be available upon request by the NIGC.
- (iii) Upon request and adequate notice by the NIGC, hardware (terminal, printer, etc.) shall be made available in order to perform auditing procedures.
- (iv) Controls shall exist to ensure the accurate reproduction of records up to and including the printing of stored documents used for auditing purposes.
- (v) The storage medium shall be retained for a minimum of five years.



Mille Lacs Band of Ojibwe Indians
Gaming Regulatory Authority
Detailed Gaming Regulations

Standards for Information Technology

Document No. DGR - 8

Effective: November 10, 2005

documentation as stated in part (i) of this section shall be submitted to the GRA Board for each new program or program change; and (iii) Testing of new and modified programs shall be performed (by the licensee or the system manufacturer) and documented prior to full implementation; Addition of section 7, Independent information technology review. Regular Gaming Enterprise information technology security risk assessments shall be conducted by external, qualified specialists at a minimum once every two (2) years; Assessments shall include, but are not limited to, a review of internal controls, identification of areas of risk, and evaluation of system and data integrity; Changes to section 8, removed modem and changed dial-up to access; Addition of section 8(A), For each computerized Gaming Enterprise application that can be accessed remotely by a vendor, the following procedures shall be maintained that include, at a minimum: (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; Changes to section 8(B), removed If remote dial-up to any associated equipment is allowed for software support and added In the event of remote access; Changes to section 8(B)(iv), added (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); and Changes to section 9, removed only citation (A) approved by the Gaming Regulatory Authority Board May 19, 2008. **Each Gaming Enterprise must come into compliance with changes no later than October 1, 2008. Effective date for changes October 1, 2008.**