NOTICE _____ OF 2002

MPUMALANGA GAMING ACT, 1995 (ACT NO. 5 OF 1995)

AMENDMENT OF MPUMALANGA GAMING RULES

General Explanatory Note:

[BOLD] words typed in bold type in square brackets indicate omissions from the existing Rules.

_____ words underlined with a solid line indicate insertions in existing Rules.

RULES

To amend the Mpumalanga Gaming Rules, 1999, so as to provide for a separate electronic data processing: EDP department; to provide for new program changes for in-house developed systems; to provide for a computerised gaming machine systems general controls; and to provide for general controls for electronic data processing and to further regulate electronic data processing modems:

Amendment of Rule 10.040 – Electronic data processing: EDP Department

1. **[If]** A separate electronic data processing (EDP) department **[is]** shall be maintained **[or if there are in-house developed computer systems]**,and the following standards shall be applicable –

   (a) the EDP department shall be independent of all gaming areas (i.e., cage, pit, count rooms, etc.);

   (b) the EDP department personnel shall be precluded from unauthorised access to computers and terminals located in gaming areas, source documents and live data files (not test data);

   [(c) 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 EDP supervisor and approvals to begin work on the program shall be documented and retained;

(ii) a written plan of implementation for new and modified programs shall be maintained and include, at a minimum, the date the program is to be 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 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; and]

[(d)] (c) computer security logs, if generated by the system, shall be reviewed by EDP supervisory personnel for evidence of –

(i) multiple attempts to log-on or, alternatively, the system shall deny user access after three attempts to log-on; and

[(ii) changes to live data files; and]

[(iii)] (ii) any other unusual transactions.

2. If there are in-house developed systems, the following standards shall be applicable –

(a) 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 EDP supervisor and approvals to begin work on the program shall be documented and retained;

(ii) a written plan of implementation for new and modified programs shall be maintained and include, at a minimum, the date the program is to be 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 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. **[and]**

Amendment of Rule 10.130 – Computerised gaming machine systems: General controls

(1) For all computerised gaming machine systems a personnel access list shall be maintained which shall include**[s]**, at a minimum, the following information –

(a) employee name;
(b) employee identification number (or equivalent); and
(c) a list of functions which that employee can perform or equivalent means of identifying same.

(2) An audit trail shall be maintained of all changes made to any individual's access to the system, which shall contain the following minimum information –

(a) the name of the person who performed the change;
(b) the name of the person who's access was changed;
(c) the nature of the change of the access;
(d) the date and time of the change;
(e) a computer generated sequential number or equivalent means of identifying same as approved by the Board; and
(f) if access rights are amended as a result of a system upgrade, these changed shall be documented.

(3) passwords shall be controlled as follows, unless otherwise addressed in the licensee's Internal Control Procedures as approved by the Board –

(a) each user shall have his or her own individual password;
(b) passwords shall be changed at least monthly; and
(c) the system shall preclude an individual from using the same password for more than one month in every twelve months.

Amendment of Rule 10.140 – Electronic data processing: General controls

The following aspects shall be addressed in the licensee's Internal Control Procedures as approved by the Board –

(a) the main computers (i.e., hardware, software and data files) for each gaming department application shall be in a secured area with access restricted to only authorised persons;

(b) gaming personnel shall be precluded from having unrestricted access to the secured computer areas;

(c) computer systems, including application software, shall be secured through the use of passwords or other approved means and access to system functions shall be controlled by management personnel or persons independent of the department being controlled;

(d) passwords shall be controlled as follows unless otherwise addressed in these standards –

(i) each user shall have his or her own individual password;
(ii) passwords shall be changed at least monthly **[with changes being documented]** and;
(iii) the system shall preclude an individual from using the same password for more than one month in every twelve months;

(e) adequate backups and recovery procedures shall be in place, and **[if applicable,]** shall include –

(i) daily 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]** backup storage devices shall be tested at least quarterly and results shall be documented and maintained; **[; and]**

(f) the licensee shall maintain written recovery plan which shall address a procedure to be followed in case of unforeseen disaster; and

[(f)] (g) adequate system documentation shall be maintained, including descriptions of both hardware and software and operator manuals.

Amendment of Rule 10.150 – Electronic data processing: Modems

If remote dial-up **[to any other gaming equipment]** is allowed for software support, the licensee shall maintain an access log which shall include the name of the employee authorising modem access, the name of the authorised programmer or manufacturer representative, the reason for modem access, a description of work performed and the date, time and duration of access.