INFORMATION TECHNOLOGY

Section 542.16 Updated through May 11, 2006

§ 542.16 What are the minimum internal control standards for information technology?

(a) *General controls for gaming hardware and software.*

(1) 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) Management shall ensure that all new gaming vendor hardware and software agreements/contracts contain language requiring the vendor to adhere to tribal internal control standards applicable to the goods and services the vendor is providing.

(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 personnel.

(iv) Access to computer data shall be limited to authorized personnel.

(v) Access to computer communications facilities, or the computer system, and information transmissions shall be limited to authorized personnel.

(vi) Standards in paragraph (a)(1) of this section shall apply to each applicable department within the gaming operation.

(2) The main computers (i.e., hardware, software, and data files) for each gaming application (*e.g.,* keno, race and sports, gaming machines, etc.) shall be in a secured area with access restricted to authorized persons, including vendors.

(3) Access to computer operations shall be restricted to authorized personnel to reduce the risk of loss of integrity of data or processing.

(4) Incompatible duties shall be adequately segregated and monitored to prevent error in general information technology procedures to go undetected or fraud to be concealed.

(5) Non-information technology personnel shall be precluded from having unrestricted access to the secured computer areas.

(6) The computer systems, including application software, shall be secured through the use of passwords or other approved means where applicable. Management personnel or persons independent of the department being controlled shall assign and control access to system functions.

(7) Passwords shall be controlled as follows unless otherwise addressed in the standards in this section.

(i) Each user shall have their own individual password;

(ii) Passwords shall be changed at least quarterly with changes documented; and

(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.

(8) 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.

(9) Adequate information technology system documentation shall be maintained, including descriptions of hardware and software, operator manuals, etc.

(b) *Independence of information technology personnel.*

(1) The information technology personnel shall be independent of the gaming areas (*e.g.,* cage, pit, count rooms, etc.). Information technology personnel procedures and controls should be documented and responsibilities communicated.
(2) Information technology personnel 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).
(3) Information technology personnel shall be restricted from:
(i) Having unauthorized access to cash or other liquid assets; and
(ii) Initiating general or subsidiary ledger entries.

(c) *Gaming program changes.*
(1) Program changes for in-house developed systems should 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 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.
(2) [Reserved]

(d) *Security logs.*
(1) If computer security logs are generated by the system, they shall be reviewed by information technology 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;
(ii) Unauthorized changes to live data files; and
(iii) Any other unusual transactions.
(2) This paragraph shall not apply to personal computers.

(e) *Remote dial-up.*
(1) If remote dial-up to any associated equipment is allowed for software support, the gaming operation shall maintain an access log that includes:
(i) Name of employee authorizing modem access;
(ii) Name of authorized programmer or manufacturer representative;
(iii) Reason for modem access;
(iv) Description of work performed; and
(v) Date, time, and duration of access.
(2) [Reserved]

(f) *Document storage.*
(1) 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 operation department and date. This index shall be available upon request by the Commission.

(iii) Upon request and adequate notice by the Commission, 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.

(2) [Reserved]

[67 FR 43400, June 27, 2002, as amended at 71 FR 27392, May 11, 2006]