

(vii) System exception information (e.g., changes to system parameters, corrections, overrides, voids, etc.) must be maintained.

(4) Procedures must be established and implemented to ensure access listings are maintained which include at a minimum:

(i) User name or identification number (or equivalent); and

(ii) Listing of functions the user can perform or equivalent means of identifying same.

(d) Adequate backup and recovery procedures must be in place that include:

(1) *Daily backup of data files*—(i) *Backup of all programs.* Backup of programs is not required if the program can be reinstalled.

(ii) Secured storage of all backup data files and programs, or other adequate protection to prevent the permanent loss of any data.

(iii) Backup data files and programs may be stored in a secured manner in another building that is physically separated from the building where the system's hardware and software are located. They may also be stored in the same building as the hardware/software as long as they are secured in a fireproof safe or some other manner that will ensure the safety of the files and programs in the event of a fire or other disaster.

(2) Recovery procedures must be tested on a sample basis at least annually with documentation of results.

(e) *Access records.* (1) Procedures must be established to ensure computer access records, if capable of being generated by the computer system, are reviewed for propriety for the following at a minimum:

- (i) Class II gaming systems;
- (ii) Accounting/auditing systems;
- (iii) Cashless systems;
- (iv) Voucher systems;
- (v) Player tracking systems; and
- (vi) External bonusing systems.

(2) If the computer system cannot deny access after a predetermined number of consecutive unsuccessful attempts to log on, the system must record unsuccessful log on attempts.

(f) *Remote access controls.* (1) For computer systems that can be accessed remotely, the written system of internal

controls must specifically address remote access procedures including, at a minimum:

(i) Record the application remotely accessed, authorized user's name and business address and version number, if applicable;

(ii) Require approved secured connection;

(iii) The procedures used in establishing and using passwords to allow authorized users to access the computer system through remote access;

(iv) The agents involved and procedures performed to enable the physical connection to the computer system when the authorized user requires access to the system through remote access; and

(v) The agents involved and procedures performed to ensure the remote access connection is disconnected when the remote access is no longer required.

(2) In the event of remote access, the information technology employees must prepare a complete record of the access to include:

(i) Name or identifier of the employee authorizing access;

(ii) Name or identifier of the authorized user accessing system;

(iii) Date, time, and duration of access; and

(iv) Description of work performed in adequate detail to include the old and new version numbers, if applicable of any software that was modified, and details regarding any other changes made to the system.

## PARTS 544-546 [RESERVED]

### PART 547—MINIMUM TECHNICAL STANDARDS FOR GAMING EQUIPMENT USED WITH THE PLAY OF CLASS II GAMES

Sec.

547.1 What is the purpose of this part?

547.2 How do these regulations affect state jurisdiction?

547.3 What are the definitions for this part?

547.4 How does a tribal government, tribal gaming regulatory authority, or tribal gaming operation comply with this part?

547.5 What are the rules of interpretation and of general application for this part?