

SUBCHAPTER 2. CASINO COMPUTER SYSTEMS

19:45-2.1 Definitions

19:45-2.2 Casino computer systems; authorized locations

19:45-2.1 Definitions

The following words and terms, when used in this chapter, shall have the following meanings unless the context clearly indicates otherwise:

“Casino computer system” means all aspects of a computer system which the rules of the Commission either require or permit to be utilized by a casino licensee in the conduct or monitoring of casino operations including, but not limited to hardware, software and network interfaces; provided, however, that a casino computer system shall not be construed to include the following:

1. A slot machine or bill changer;
2. A multi-casino progressive slot system;
3. A computer system that is connected to a casino computer system only through a firewall, which has been approved in accordance with the provisions of N.J.A.C. 19:46-1.20 and for which the casino licensee has approved internal controls in accordance with the requirements of N.J.A.C. 19:45-2.2(g); and
4. Any computer system used exclusively in the conduct of casino simulcasting, in accordance with the provisions of N.J.A.C. 19:55.

“Computer access” or “logical access” means the ability of a person or process to obtain information from, or execute an action in, a casino computer system in accordance with privileges established by a casino licensee pursuant to approved internal controls, which privileges shall be specified by an approved level of computer access.

“Computer functionality” means that a casino computer system functions as designed and approved.

“Computer security” means that a casino computer system contains sufficient devices or procedures that shall:

1. Preserve computer functionality, availability, and the confidentiality of data in accordance with the requirements of the Act and the Commission's rules;

2. Appropriately limit the ability of any person or process to deliberately or inadvertently interfere with the normal operation of the system or its data; and

3. Detect, record, preserve, and provide notice to the casino licensee of, in accordance with approved internal controls, each compromise, possible compromise, inadvertent disclosure, or deviation from computer functionality that occurs.

“Firewall” means dedicated computer hardware, software, and the related security policy that protects a casino computer system, its software, and data from access by other computer systems and users not specifically authorized to access the casino computer system, its software or data, through procedures approved by the Commission, such as monitoring and analyzing all data packets on a real-time basis and automatically rejecting all unauthorized communications. A firewall shall include, without limitation, logging and reporting, automatic alarms, and a user interface for controlling the firewall.

“Level of computer access” means the particular privileges granted to a person in a casino computer system by a casino licensee, such as read, read-write, execute, and modify, which privileges shall vary by casino computer system program, process, library, or directory, according to the following:

1. Position title and job code, for an employee of the casino licensee; and

2. Responsibilities and functions authorized to be performed, for any person not employed by the casino licensee.

Adopted effective: 07/05/05

19:45-2.2 Casino computer systems; authorized locations

(a) All aspects of a casino licensee's casino computer system shall be located within the casino hotel facility unless otherwise approved by the Commission in accordance with the provisions of this section.

(b) The Commission may permit a casino licensee to maintain the software and data of its casino computer system, or any portion thereof, in a computer located in a secure location outside the casino hotel facility, referred to herein as a "remote computer", provided that:

1. The remote computer is maintained in a secure location within the casino hotel facility of another casino licensee, referred to herein as a "host casino", except as otherwise permitted by the Commission in the event of a disaster pursuant to (e) below;

2. Communications between the remote computer and all other portions of the casino computer system shall occur using a dedicated and secure communication facility, such as a leased line, as approved by the Commission;

3. The remote computer shall automatically perform, at a minimum, the following functions:

i. Generate daily monitoring logs and real time alert messages to inform the casino licensee, host casino, or both, of any system performance problems and hardware problems;

ii. Generate daily monitoring logs and real time alert messages to inform the casino licensee of any software errors;

iii. Generate daily monitoring logs to inform the casino licensee of any unsuccessful attempts by a device, person or process to obtain computer access;

iv. Authenticate the identity of each device, person and process from which communication is received before granting computer access to such device, person or process;

v. Ensure that data sent through a transmission is

completely and accurately received; and

vi. Detect the presence of corrupt or lost data and, as necessary, reject the transmission; and

4. Unless a remote computer is used exclusively to maintain a casino computer system of one casino licensee, it shall be partitioned in a manner approved by the Commission, and shall include, at a minimum, the following:

i. A partition manager that complies with the following requirements:

(1) The partition manager shall be comprised of hardware and/or software and shall perform all partition management tasks for a remote computer, including creating the partitions described in (b)4ii below and allocating system resources to each such partition, such as processors, communication buses, data storage devices, and memory;

(2) The casino licensee and host casino shall jointly designate and each shall identify in its approved internal controls the MIS security officer who shall be responsible for administering the partition manager and maintaining access codes to the partition manager, which MIS security officer shall be an employee of the casino licensee, host casino, or any holding, intermediary or subsidiary company thereof;

(3) Special rights and privileges in the partition manager such as “administrator” shall be restricted to the MIS department manager and the MIS security officer of the casino licensee, host casino, or any holding, intermediary or subsidiary company thereof, provided, however, that such rights and privileges may be delegated in accordance with N.J.A.C. 19:45-1.11(b)3; and

(4) Access to the partition manager shall be limited to employees of the MIS departments of the casino licensee, host casino, or any holding, intermediary or subsidiary company thereof, unless otherwise approved by the Commission; and

(5) Software-based partition managers contained in a remote computer shall be functionally limited to performing partition management tasks for the remote computer, while partition managers using hardware and software that are not part of a remote computer may be utilized to perform other functions for a remote computer that are approved by the Commission;

ii. A separate and distinct partition for each casino computer system that complies with the following requirements:

(1) The partition shall be limited to maintaining the software and data of the casino licensee or affiliate for which the partition has been established;

(2) The MIS security officer of the casino licensee for which the partition has been established shall be responsible for maintenance of access codes to the partition;

(3) Special rights and privileges in the partition such as “administrator” shall be restricted to the MIS security officer and the MIS department manager of the casino licensee for which the partition has been established, provided, however, that such rights and privileges may be delegated in accordance with N.J.A.C. 19:45-1.11(b)3; and

(4) A partition shall not utilize or share a processor, communication bus, data storage device, and memory that is not partitioned or otherwise segregated from the partition manager and any other partition, in a manner approved by the Commission; and

iii. Separate and distinct operating system software, application software, and computer access controls for the partition manager and each partition required in accordance with the provisions of (b)4i and ii above.

(c) The Commission may permit a casino licensee to establish a partition, within a computer that contains a casino computer system, for any holding, intermediary or subsidiary company thereof, or any affiliate that holds a gaming license in any other jurisdiction in the United States, in accordance

with the requirements of (b)4ii(1) and (4), and (b)4iii above.

(d) The Commission may permit a casino licensee to maintain duplicate copies of the software and data of a casino computer system, or any portion thereof, in removable storage media devices, such as magnetic tapes or disks, which reside in a secure location within the casino hotel facility or such other secure location outside the casino hotel facility within the State of New Jersey approved by the Commission, for the purposes of disaster recovery.

(e) Notwithstanding the provisions of (b) above, a casino licensee may maintain the software and data of its casino computer system, or any portion thereof, in a computer located in a secure location outside the casino hotel facility, only upon the declaration of a disaster affecting the casino computer system by the chief executive officer of the casino licensee and prior approval of the Commission.

(f) A casino licensee may locate software or data not related to a casino computer system, such as hotel-related software or data, in a computer located outside the casino hotel facility. The Commission may permit a casino licensee to connect such computer to a casino computer system, provided that:

1. Logical access to computer software and data of the casino computer system is appropriately limited as set forth in the casino licensee's approved internal controls; and

2. Communications with all portions of the casino computer system shall occur as follows:

- i. Using a dedicated and secure communication facility, such as a leased line, as approved by the Commission; and

- ii. Only through a firewall or other comparable hardware and software, which has been approved in accordance with the provisions of N.J.A.C. 19:46-1.20 and for which the casino licensee has approved internal controls in accordance with the requirements of (g) below.

(g) Each firewall or comparable hardware and software required in accordance with the provisions of (b)3 or (f)2ii above shall perform the

following:

1. Maintain a list of each device, person or process authorized to obtain computer access;
2. Generate daily monitoring logs to inform the casino licensee of any unsuccessful attempts by a device, person or process to obtain computer access; and
3. Authenticate the identity of each device, person and process from which communication is received before granting computer access to such device, person or process.

Adopted effective: 07/05/05