

**112-107-20. EGM computer systems.** (a) All components of a facility manager's production EGM computer system shall be located within the gaming facility. As used in this regulation, "production EGM computer system" shall mean the facility manager's primary EGM computer system comprised of a collection of hardware and software used to process or monitor EGM activity in real time. A production EGM computer system shall include any segregated testing component.

(b) With the written approval of the executive director, a facility manager's back-up EGM computer system, or any part of it, may be located in a secure and remote computer that is under the custody and control of an affiliate, intermediary, subsidiary, or holding company approved by the commission, referred to as a "host entity." A backup EGM computer system may consist of either of the following:

(1) A mirrored backup system that duplicates the production system by recording all slot-related operations on a real-time basis and is designed to become the production system whenever needed; or

(2) a periodic backup system that consists of regularly scheduled recording of selected data, which may include a complete image of the production system or any portion of the system.

(c) At a minimum, each facility manager requesting authorization to allow a backup EGM computer system to reside outside the gaming facility shall certify that both of the following conditions are met:

(1) Communications between the remote computer and the facility manager's EGM computer system occur using a dedicated and secure communication medium, which may include a leased line.

(2) The remote computer automatically performs the following functions:

(A) Generates daily monitoring logs and real-time alert messages to inform the facility manager and host entity of any system performance problems and hardware problems;

(B) generates daily monitoring logs and real-time alert messages to inform the facility manager of any software errors;

(C) generates daily monitoring logs to inform the facility manager of any unsuccessful attempts by a device, person, or process to obtain computer access;

(D) authenticates the identity of every device, person, and process from which communications are received before granting computer access to the device, person, or process;

(E) ensures that data sent through a transmission is completely and accurately received; and

(F) detects the presence of corrupt or lost data and, as necessary, rejects the transmission.

(d) Unless a remote computer is used exclusively to maintain the EGM computer system of the facility manager, the system shall be partitioned in a manner approved by the executive director and shall include the following:

(1) A partition manager that meets the following requirements:

(A) The partition manager shall be comprised of hardware or software, or both, and perform all partition management tasks for a remote computer, including creating the partitions and allocating system resources to each partition;

(B) the facility manager and host entity shall jointly designate and identify the security officer who will be responsible for administering the partition manager and maintaining access codes to the partition manager. The security officer shall be an employee of the facility manager or host entity and shall be licensed as a level I employee;

(C) special rights and privileges in the partition manager, including the administrator, shall be restricted to the management information systems director or security officer of the facility manager or host entity, who shall be licensed as level I employees;

(D) access to the partition manager shall be limited to employees of the management information systems departments of the facility manager and host entity; and

(E) 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 executive director;

(2) a separate partition established for the facility manager's EGM computer system that meets the following requirements:

(A) The partition shall be limited to maintaining the software and data of the facility manager for which the partition has been established;

(B) the security officer of the facility manager for which the partition has been established shall be licensed as a level I employee and shall be responsible for maintenance of access codes to the partition; and

(C) special rights and privileges in the partition, including the administrator, shall be restricted to the security officer and the management information systems director of the facility manager for which the partition has been established; and

(3) separate and distinct operating system software, application software, and computer access controls for the partition manager and each separate partition.

(e) Any facility manager may be permitted by the executive director to establish a partition within a computer that contains its EGM computer system for its affiliate, intermediary, subsidiary, or holding company if all of the following requirements are met:

(1) A partition manager comprised of hardware or software, or both, shall be utilized to perform all partition management tasks, including creating the partitions and allocating system resources to each partition.

(2) A security officer shall be designated within the management information systems department of the facility manager to be responsible for administering the

partition manager and maintaining access codes to the partition manager. Special rights and privileges in the partition manager, including the administrator, shall be restricted to the security officer and the management information systems director of the facility manager.

(3) Special rights and privileges in any partition that has been established for the benefit of an affiliate, intermediary, subsidiary, or holding company shall be restricted to the security officer and information technology director of the affiliate, intermediary, subsidiary, or holding company.

(f) Any facility manager may be permitted by the executive director to maintain backup or duplicate copies of the software and data of its EGM computer system, or any portion of the software and data, in removable storage media devices, including magnetic tapes or disks, in a secure location within a gaming facility or other secure location outside the gaming facility as approved by the executive director for the purposes of disaster recovery.

(g) Notwithstanding the provisions of subsection (a), upon the declaration of a disaster affecting the EGM computer system by the chief executive officer of the facility manager and with the prior written approval of the executive director, a facility manager may maintain the software and data of its EGM computer system, or any portion of the software and data, in a computer located in a secure location outside the gaming facility.

(h) Any facility manager may locate software or data not related to an EGM computer system, including software or data related to the sale of food and beverages, in

a computer located outside the gaming facility. With the written approval of the executive director, a facility manager may connect the computer to an EGM computer system if all of the following conditions are met:

(1) Logical access to computer software and data of the EGM computer system is appropriately limited.

(2) Communications with all portions of the EGM computer system occur using a dedicated and secure communications medium, which may consist of a leased line.

(3) The facility manager complies with other connection-specific requirements of the commission. (Authorized by and implementing K.S.A. 2007 Supp. 74-8772; effective April 24, 2009.)