

CHAPTER 461b. REMOTE COMPUTER ACCESS—TECHNICAL STANDARD

§ 461b.5. Remote computer access.

(a) In emergency situations or as an element of technical support, an employee of a licensed manufacturer may perform analysis of, or render technical support with regard to, a slot machine licensee's slot monitoring system, casino management system, player tracking system, external bonusing system, cashless funds transfer system, wide area progressive system, gaming voucher system or other approved system from a remote location. Any remote access to these systems shall be performed in accordance with the following procedures:

(1) Only an employee of a licensed manufacturer who is licensed as a gaming employee or key employee in this Commonwealth may remotely access a system sold, leased or otherwise distributed by that licensed manufacturer for use at a licensed facility.

(2) The slot machine licensee shall establish a unique system account for each employee of a licensed manufacturer identified by his employer as potentially required to perform technical support from a remote location. Any system access afforded pursuant to this section must:

(i) Be restricted in a manner that requires the slot machine licensee's information technology department to receive prior notice from the licensed manufacturer of its intent to remotely access a designated system.

(ii) Require the slot machine licensee to take affirmative steps, on a per access basis, to activate the licensed manufacturer's access privileges.

(iii) Be designed to appropriately limit the ability of any person authorized under this section to deliberately or inadvertently interfere with the normal operation of the system or its data.

(3) A log shall be maintained by both the licensed manufacturer and the slot machine licensee's information technology department. Each of the two logs must contain, at a minimum, the following information:

(i) The system accessed, including manufacturer and version number.

(ii) The type of connection (that is, leased line, dial in modem or private WAN).

(iii) The name and license number of the employee remotely accessing the system.

(iv) The name and license number of the information technology department employee activating the licensed manufacturer's access to the system.

(v) The date, time and duration of the connection.

(vi) The reason for the remote access including a description of the symptoms or malfunction prompting the need for remote access to the system.

(vii) Any action taken or further action required.

(4) Communications between the licensed manufacturer and any of the systems identified in subsection (a) shall occur using a dedicated and secure communication facility such as a leased line approved in writing by the Board.

(b) Any modification of, or remedial action taken with respect to, an approved system must be processed and approved by the Board either in accordance with the emergency modification provisions of § 461a.4(l) (relating to submission for testing and approval) or as a standard modification submitted under § 461a.4(h).

(c) If an employee of a licensed manufacturer is no longer employed by, or authorized by, that manufacturer to remotely access a system pursuant to this section, the licensed manufacturer shall immediately notify the Board's Slot Lab and each slot machine licensee that has established a unique system account for that employee of the change in authorization and shall timely verify with each slot machine licensee that any access privileges previously granted have been revoked.

(d) The Board may waive one or more of the technical requirements applicable to remote computer access adopted by the Board upon a determination that the nonconforming remote access procedures nonetheless meet the integrity requirements of the act, this part and technical standards adopted by the Board.