NEW SECTION

WAC 230-16-153 Remote access of electronic raffle systems. Electronic raffle systems may be accessed remotely, at any time, only by a licensed representative of the manufacturer of the equipment for repair, troubleshooting, or technical support under the following provisions:

(1) In order to be approved to remotely access the electronic raffle system, the manufacturer must:

(a) Submit an application and documentation as required in WAC 230-06-050; and

(b) Have the remote access solution tested. This may be done by:

(i) Submitting and transporting a working model of the remote access solution and related documentation, in the format we require, to us for testing and approval; or

(ii) Have the remote access solution tested on-site by us; and

(2) For the purpose of continued monitoring, we may retain a working model or components after approval for as long as the remote access solution is in use in the state; and

(3) The manufacturer must notify and receive approval from the electronic raffle licensee before remotely accessing the electronic raffle system for the reasons outlined above; and

(4) The manufacturer must notify us within 24 hours after the remote access has occurred; and

(5) The remote access must occur using a dedicated and secure communication protocol or application utilizing encryption such as a virtual private network (VPN); and

(6) The remote access must only be conducted through a laptop or computer owned and issued by the manufacturer and must meet the following requirements:

(a) Employ full disk encryption; and

(b) Have a mechanism to detect and prevent installation of spyware, key loggers, hacking tools, or other malicious software; and

(c) Have current updated antivirus software; and

(d) Employ active firewall software; and

(e) Be conducted in a secure location where only the manufacturer or licensed representatives can be present while accessing the electronic raffle system remotely; and

(7) All remote access to the electronic raffle system must use multifactor authentication; and

(8) The communication must pass through at least one application-level firewall and not have the ability to allow for an alternate network path; and

(9) Remote access shall only be enabled for the duration of repair, troubleshooting, or technical support and the connection terminated immediately after; and

(10) Security standards for the remote access must be at least equivalent to commonly accepted national and international best practices for IT security such as National Institute of Science and Technology (NIST) standards as they currently exist or may be amended in the future; and

(11) An electronic log shall be maintained by the electronic raffle system for documentation and audit purposes and must include the following information about all remote access to the electronic raffle system:

(a) Name and license number of manufacturer representative that accessed the system; and

(b) Time and date the connection was made; and

(c) Duration of the connection; and

(d) Reason for the remote access; and

(e) Any action taken, or further action required; and

(12) The manufacturer must disable access for an employee that is no longer with the company within 24 hours of termination.