

WAC 230-15-773 Requirements for ticket validation system. Ticket validation systems must:

- (1) Not use, permit the use of, validate, or redeem tickets issued by another licensee; and
- (2) Be able to identify invalid tickets and issued tickets, and notify the cashier, dealer, or kiosk, which is applicable, if:
 - (a) The validation number cannot be found; or
 - (b) The ticket has already been redeemed; or
 - (c) The amount on file for the ticket does not match; and
- (3) Uniquely identify TITO-enabled bill validators and ticket redemption kiosks connected to it; and
- (4) Be able to generate the following reports to be reconciled with all validated/redeemed tickets:
 - (a) Ticket issuance report; and
 - (b) Ticket redemption report; and
 - (c) Ticket liability report; and
 - (d) Ticket drop variance report; and
 - (e) Transaction detail report that shows all tickets generated and redeemed by a TITO-enabled bill validator and ticket redemption kiosk; and
 - (f) Cashier report, which is to detail individual tickets and the sum of tickets paid by a cage cashier or ticket redemption kiosk; and
- (5) Employ encryption standards suitable for the transmission and storage of all confidential or sensitive information between all components of the system; and
- (6) Not allow for any wireless connections or communication; and
- (7) Can only be connected to authorized gambling equipment; and
- (8) Have all servers and components that store sensitive information in a locked secure enclosure with both camera coverage and key controls in place; and
- (9) Have a machine entry authorization log (MEAL) for all entries into a locked area that indicates the date, time, purpose of entering the locked area(s), and the name and employee number of the employee doing so; and
- (10) Maintain an internal clock that reflects the current time and date that shall be used to provide the following:
 - (a) Time stamping of significant events; and
 - (b) Reference clock for reporting; and
 - (c) Time stamping of configuration changes; and
- (11) Have a recent backup that is securely stored, separate from the system, in case of catastrophic failure and the ticket validation system cannot be restarted. Backups must be retained for a period of at least two years. Backups must contain:
 - (a) Significant events; and
 - (b) Accounting information; and
 - (c) Auditing information; and
 - (d) All information utilized in the ticket redemption and issuance process; and
- (12) Be connected to a device that provides surge protection and a temporary power source, such as a uninterruptible power supply (UPS), to provide a means for an orderly shutdown in the event of a main power system failure; and
- (13) Have no built-in facility where a casino user/operator can bypass system auditing to modify any database(s) directly; and
- (14) Log any changes made by a user to accounting or significant event log information that was received from a device on the system. The log must include:

- (a) Date data was altered; and
- (b) Value prior to alteration; and
- (c) Value after alteration; and
- (d) Identification of personnel that made the alteration; and

(15) Record significant events generated by any TITO devices on the system. Each event must be stored in a database(s) and include the following information:

- (a) Date and time the event occurred; and
- (b) Identify the device that generated the event; and
- (c) A unique number/code that identifies the event; and
- (d) A brief text that describes the event in the local language;

and

(16) Have a means by which any user accessing the system software, either by password, keycard, or PIN have a username or user number unique to that individual and log the date and time of access.

[Statutory Authority: RCW 9.46.070. WSR 23-20-017, § 230-15-773, filed 9/22/23, effective 10/23/23.]