Ohio Administrative Code

Rule 3775-9-02 Sports gaming systems.

Effective: August 15, 2022

(A) A sports gaming system must monitor and record all data related to sports gaming in real-time, including any changes made to the data or system. The sports gaming system must provide accurate reporting using a method and format approved by the executive director.

(B) A sports gaming system must be capable of automatically preparing a report summarizing the results of all sports gaming transactions conducted in this state. The report must be tested by a certified independent testing laboratory to confirm that it accurately calculates and displays the results of sports gaming. The format and the required periods of this report are determined by the executive director.

(C) The sports gaming system servers, or other equipment, responsible for accepting wagers must be located within the state of Ohio. This rule does not prohibit sports gaming data from being stored or accessed elsewhere, including cloud-based environments.

(D) The sports gaming system servers or other equipment required to be located in Ohio, under paragraph (C) of this rule, must be managed by an entity holding a sports gaming proprietor or sports gaming supplier license. The data center where the sports gaming system server is housed must be secure and have access controls in place to prevent unauthorized access to the sports gaming system servers or other equipment.

(E) Sports gaming systems must utilize disk redundancy and sports gaming data must be backed up to prevent the loss of data and minimize down time.

(F) All communication with a sports gaming system must be secured utilizing an encryption methodology that ensures data integrity and prevents data theft.

(G) The sports gaming system must perform an authentication check on any sports gaming equipment which connects to it. The sports gaming system must not accept any wagers or player

account requests from sports gaming equipment that fails the authentication check. The authentication check must:

(1) Occur at least once every twenty-four hours;

(2) Determine with a high degree of accuracy if the sports gaming equipment has been altered in a way that may threaten the integrity of the sports gaming system or data; and

(3) Be logged, including, but not limited to:

(a) Date and time;

(b) Device identifier;

(c) Device type;

(d) Location; and

(e) Disposition of the authentication check.