TITLE 11—DEPARTMENT OF PUBLIC SAFETY
Division 45—Missouri Gaming Commission
Chapter 20—Sports Wagering

PROPOSED RULE

11 CSR 45-20.220 Information Technology

PURPOSE: This rule establishes requirements for information technology for Retail and Mobile licensees.

(1) Retail licensees and Mobile licensees shall have an information technology department that is responsible for the quality, reliability, and accuracy of all computer systems used in the sports wagering operation. Information technology functions shall only be outsourced to SW Supplier licensees.

(2) Each individual who has write access to the sports wagering system shall possess a commission-issued SW Occupational license, unless otherwise approved in writing by the commission.

(3) Retail licensees and Mobile licensees shall ensure that duties in the information technology department are adequately segregated and monitored to detect procedural errors, unauthorized access to financial transactions and assets, and to prevent the concealment of fraud.

(4) The information technology environment and infrastructure shall be maintained in a secured physical location, which may include but is not limited to a comprehensive cloud computing platform or data center, that is restricted to authorized employees.

(5) Retail licensees and Mobile licensees shall adopt procedures in the internal controls for responding to, monitoring, investigating, resolving, documenting, and reporting security incidents associated with information technology systems.

(6) System enforced security parameters for passwords shall be documented in the Retail licensee’s or Mobile licensee’s internal control system and meet industry standards.

(7) Each user account in the sports wagering system shall be assigned to an individual and shall not be made available or used by any other individual. The individual assigned to the user account will be held responsible for all activities performed under that individual’s user account.

(8) A system administrator shall establish all user accounts. Each account shall only provide access consistent with the employee's current job responsibilities as delineated in the employee's job description. The access shall maintain proper segregation of duties and restrict unauthorized users from viewing, changing, or deleting critical files and directories.

(9) Anytime an employee transfers to a new position, the employee’s account(s) shall be reviewed and adjusted within seventy-two (72) hours of the change in position to align with the requirements

of the new position. Any access no longer required for the new position shall be removed prior to granting new access privileges.

(10) Retail licensees and Mobile licensees shall generate on request user access listings, which shall include at a minimum:

(A) Employee name;
(B) Title, position, or job group;
(C) User login name;
(D) Full list and description of application functions that each group/user account may execute;
(E) Date and time account created;
(F) Date and time of last login;
(G) Date of last password change;
(H) Date and time account disabled/deactivated; and
(I) Group membership of user account, if applicable.

(11) When multiple user accounts for one (1) employee per application are used, only one (1) user account shall be active (enabled) at a time, if the concurrent use of the multiple accounts by the employee could create a segregation of duties deficiency. Additionally, the user account shall have a unique prefix/suffix to easily identify the users with multiple user accounts within one (1) application.

(12) The information technology department shall be notified upon termination of any employee who has access to the sports wagering system. The terminated employee's user account(s) shall be disabled or deactivated within seventy-two (72) hours of termination or suspension subject to termination; or if the user account has remote access, the account shall be disabled by the end of the next calendar day.

(13) Except when a Retail licensee or Mobile licensee implements multi-factor authentication controls, user accounts shall be automatically locked out after at most five (5) failed login attempts. The system may release a locked out account after thirty (30) minutes have elapsed.

(14) All user and system accounts shall be logged out or the screen shall be locked after fifteen (15) minutes of inactivity.

(15) Employees shall only access the sports wagering system using their own username and password, which shall not be shared with or used by any other person.

(16) All passwords shall be encrypted during electronic transmission and storage in the sports wagering system.

(17) Generic user accounts shall be read-only. Generic user accounts are accounts that are shared by multiple users and are not assigned to an individual. Service accounts, on which automated system functions are executed, are not considered generic accounts for the purpose of this rule.

(18) Retail licensees and Mobile licensees shall maintain a backup of all data related to sports wagering. The commission may approve the use of cloud storage located in the United States for duplicated data upon written request by the licensee.

(19) Information technology employees shall test the recovery procedures of the sports wagering system on a sample basis at least once every six (6) months. The results shall be documented and available to the commission upon request.

AUTHORITY: section 39(g) of Article III, Mo. Const., sections 313.004 and 313.800–313.850, RSMo 2016 and Supp. 2024. Original rule filed May 14, 2025.