Ohio Lottery Commission

Minimum **I**nternal **C**ontrols **S**tandards
IT-Information Technology
Sports Gaming

INFORMATION TECHNOLOGY

Note 1: Unless otherwise specified, all Information Technology (IT) MICS apply to Lottery sports gaming proprietors (LSGP) applications, and the underlying databases and operating systems.

Note 2: NOT APPLICABLE

Note 3: NOT APPLICABLE

Note 4: NOT APPLICABLE

Note 5: NOT APPLICABLE

Note 6: Definitions - The following terminology and respective definitions are used in these MICS unless the context requires otherwise:

Backup system log - is an event log, a job log, or an activity file created by the program or batch process that performs backups of application and data files. These event logs, job logs, or activity files usually provide detail on the type of backup performed, success or failure of the operation, and a list of errors.

Cloud computing service provider - is a person who, on behalf of a LSGP, provides cloud computing services by acquiring and maintaining the computing infrastructure and software necessary to provide cloud computing services for associated equipment, cashless wagering systems, games, gaming devices, sports gaming operations, in whole or in part, and otherwise in accordance with Ohio Rules 3770 and 3775

Critical IT systems and equipment - includes all components of systems hardware and software, application software, and database software that individually or in combination are necessary for the stable operation of sports gaming systems. The term does not include wagering devices or kiosks.

Default accounts - are user accounts with predefined access levels usually created by default at installation for operating systems, databases, and applications. These accounts tend to be used for training purposes.

Generic user accounts - are user accounts that are shared by multiple users (using the same password) to gain access to sports gaming and applications systems (e.g., type c host login for point of sale, cashing, etc.). User accounts established by/for and used by manufacturers of the system for vendor support purposes are not considered to be generic accounts.

Group membership - (group profile) is a method of organizing user accounts into a single unit (by job position) whereby access to application functions may be modified at the unit level and the changes take effect for all user accounts assigned to the unit. A user account may be assigned to one or more groups.

Hosting center - means a facility hosting on its premises any part(s) of Lottery regulated hardware or software. The term does not include a type C host partner location.

IT personnel - are employees of the LSGP/operator or an IT service provider who are independent of the LSGP and have been designated to perform the information technology function for the operation of critical IT systems and equipment. The term is not limited to employees within an IT department, provided that the employee has sufficient training and knowledge.

INFORMATION TECHNOLOGY

IT service provider - is a person engaged by the LSGP to provide system management, system administration, user access administration, support, security, or disaster recovery services to the LSGP.

Physical and logical segregation of the development and testing from the production environment - is separating the development and testing of new software in an environment that is isolated from the regular production (live) network. The development environment is located on a separate server and developers are precluded from having access to the production environment.

Secured repository - is a secured environment that is used to store software source code once it has been approved for introduction into the production (live) environment. The repository is secured such that developers cannot modify code once it has been stored. In this way, the repository provides a history of a given software system ordered by version.

Service accounts - are accounts on which automated system functions (services) are dependent to execute. A service account does not correspond to an actual person. These are often built-in accounts that an automated system function (service) uses to access resources they need in order to perform its activities. However, some automated functions may require actual user accounts to perform certain functions and may be employed using domain accounts to run services.

System administrator - is the individual(s) responsible for maintaining the stable operation of the IT environment (including software and hardware infrastructure and application software) and/or has system authorization access to perform the following administrative function(s) for the LSGP:

i. Add, change, or delete user accounts and associated user provisioning for database, operating system, and network layers (may also include user access administrator function for an application layer).
ii. Modify operating system, database, and application security and policy parameters;
iii. Add, change, or delete system exception logging information; or
iv. Add, change, or delete permissions to data files and folders.

User access administrator - is the individual(s) responsible for and has system authorization access to add, change, or delete user accounts and associated user provisioning. User provisioning consists of assigning application functions matching the employee's current job responsibilities, unless otherwise authorized by management personnel, to ensure adequate segregation of duties.

INFORMATION TECHNOLOGY

Service Providers

Note: The employee responsible for the documentation required by MICS #1 through #3 must be delineated within the written system of internal control . The documentation is to be made available upon request by authorized internal and external auditors and by the Lottery.

1. If an IT service provider is used for LSGP operations , including the underlying databases and operating systems, documentation is maintained delineating at a minimum:

   a. The name(s) of the IT service provider used;

   b. The service(s) that are provided by the IT service provider (e.g., backup and recovery, user provisioning, or maintenance of the system); and

   c. The designation and identification of one or more management officials having primary responsibility for managing the relationship with the IT service provider.

   Note: The LSGP written system of internal control is to identify the IT service provider and is to delineate the IT functions performed by the IT service provider to comply with IT MICS. The LSGP remains ultimately responsible to ensure the proper design and implementation of the procedures required to meet all applicable IT MICS, regardless of who is performing the IT function.

2. If a cloud computing service provider is used for associated equipment, cashless wagering systems, games, gaming devices, LSGP operations in whole or in part, documentation is maintained delineating at a minimum:

   a. The name of the cloud computing service provider used;

   b. The services that are provided by the cloud computing service provider (i.e., Software as a Service, Platform as a Service, or Infrastructure as a Service);

   c. List of associated equipment, cashless wagering systems, games, gaming devices, LSGP operations, in whole or in part, for which the cloud computing service is provided;

   d. The type of cloud deployment model (e.g., private cloud, community cloud, or public cloud);

   e. The designation and identification of one or more management officials having primary responsibility for managing the relationship with the cloud computing service provider; and

   f. The contracts/agreements between the LSGP and the cloud computing service provider shall be maintained and available for review by the Lottery.

3. Documentation is maintained delineating the policies and procedures established to ensure oversight by LSGP personnel when a cloud computing service provider is used. The employee responsible for the documentation indicating the procedures must be delineated within the written system of internal control. The noted documentation must be made available upon request by authorized internal and external auditors and by the Lottery

Note: Procedures may include, but are not limited to, changes made to the systems or notification of security incidents.

Physical Access and Maintenance Controls

Note: If a cloud computing service provider is utilized, the procedures in place by the cloud service provider must provide the same level of control as required by this section to ensure the critical IT systems and equipment for each gaming application are maintained in a secured area and restricted to authorized personnel.

4. The critical IT systems and equipment for each LSGP are maintained in a secured area (secured area includes a hosting center). The area housing the critical IT systems and equipment are equipped with the following:

   a. Redundant power sources to reduce the risk of data loss in case of interruption of power.

   Note: MICS #4(a) does not apply to components in the kiosk or wagering device cabinet

   b. Adequate security mechanisms, such as traditional key locks, biometrics, combination door locks, or an electronic key card system to prevent unauthorized physical access to areas housing critical IT systems..

   c. The administration of the electronic security systems, if used to secure areas housing critical IT systems and equipment, is performed by personnel independent of the LSGP

   Note: The written internal control pursuant to operating standards and rules must delineate the methods, processes and practices used for meeting MICS#4 (a-c).

5. Access to areas housing critical IT systems and equipment for sports gaming is restricted to authorized IT personnel. LSGP personnel, including the manufacturers of the gaming computer equipment, are only allowed access to the areas housing critical IT systems when authorized by IT personnel and with periodic monitoring by IT personnel during each access.

6. A record of each access described in the previous standard by non-IT personnel, including the personnel of the manufacturer of the system, is maintained and includes at a minimum:

   a. The name of the visitor(s);

   b. Time and date of arrival;

   c. Time and date of departure;

   d. Reason for visit; and

   e. The name of IT personnel authorizing such access.

   Note: The items required by #6(d) and #6(e) can be documented on a separate log (e.g., help desk ticket).

INFORMATION TECHNOLOGY

System Parameters

Note: For MICS #7 through #10 the written system of internal control, is to delineate separately for each layer of the system (application, operating system, database, and network, where applicable) whether the system is configurable and to what extent.

7. The computer systems, including sports gaming related application software, are logically secured through the use of passwords, biometrics, or other means approved by the Lottery . Security parameters for passwords shall meet the following minimum requirements:

   a. Passwords are changed at least once every 90 days.

   b. Passwords are at least 8 characters in length and contain a combination of at least two of the following criteria: upper case letters, lower case letters, numeric and/or special characters.

   c. Passwords may not be re-used for a period approved by the Lottery or passwords may not be re-used within the last ten password changes.

   d. User accounts are automatically locked out after five (5) failed login attempts.

   Note: MICS #7 does not apply to service accounts and generic user accounts (e.g., host logins for point of sale, cashing, etc.).

8. A system event log or series of reports/logs for operating systems (including the database and network layers where applicable) and gaming , if capable of being generated by the system, is configured to track the following events:

   a. Failed login attempts.

   Note: If configurable by the system, parameters may be set so that only certain attempts are flagged for review (e.g., failed login attempts exceeding a certain number or failed login attempts to a specific address are flagged for review).

   b. Changes to live data files occurring outside of normal program and operating system execution.

   Note: Databases and operating systems are to be configured to monitor for and record manual edits and modifications made by users (not automatically by programs or operating systems) to data files and database tables belonging to sports gaming systems..

   c. Changes to operating system, database, network, and application policies and parameters.

   Note: Policies and parameters include, but are not limited to:

   i. Audit settings (types of events that are monitored and logged)
   ii. Password complexity settings (minimum length, maximum age, etc.)
   iii. System security levels (AS/400, QSecurity)
   iv. Point structure in players club systems

d. Audit trail of information changed by administrator accounts. Information logged is to include the events related to the functions described in the definitions of "system administrator" and "user access administrator". Administrator account activity logs, if provided by the system, are to include:

   i. Account login name;
   ii. Date and time of event;
   iii. Description of event;
   iv. Value before the change; and
   v. Value after the change.

e. Changes to date/time on master time server.

9. Exception reports (for application level only), if capable of being produced by the system, (e.g., changes to system parameters, corrections, overrides, voids, or wagering account adjustments) for each sports gaming systems are maintained and include at a minimum:

   a. Date and time of alteration;

   b. Identification of user that performed alteration;

   c. Data or parameter altered;

   d. Data or parameter value prior to alteration; and

   e. Data or parameter value after alteration.

10. User access listings include, if the system is capable of providing such information, at a minimum:

   a. Employee name and title or position.

   b. User login name.

   c. Full list and description of application functions that each group/user account may execute.

   Note: This list for MICS #10(c) may be available in a separate report if the menu functions are easily referenced between the user access listing report and the menu function report.

   d. Date and time account created.

   e. Date and time of last login.

   f. Date of last password change.

   g. Date and time account disabled/deactivated.

   h. Group membership of user account, if group membership is used in the system.

Note: NOT APPLICABLE

Event Log Review

11. Logs for the events listed in MICS #8(a) through (c) and (e) are to be maintained by a LSGP for a minimum of seven (7) days; the logs in MICS #8(d) are to be maintained for a minimum of 30 days.

12. Daily system event logs are reviewed at least once a week (for each day of the entire previous week) by IT personnel for events listed in MICS #8. The employee(s) responsible for reviewing the system event logs must be delineated within the written system of internal control . The results of the review must be documented (e.g., log, checklist, or notation on reports) and maintained. The documentation is to include:

    a. Date and time of review;

    b. Name and title of individual performing the review;

    c. Details of any exceptions noted; and

    d. Follow-up and resolution of exceptions.

    Note 1: For this standard an automated tool that polls the event logs for all sports gaming servers and provides the reviewer with notification of the above may be used. Maintaining the notification may serve as evidence of the review, provided that the date, time, name of individual performing the review of the exceptions noted, and any follow-up of the noted exception are documented in the notification or in a separate document maintained as required by this standard.

    Note 2: The LSGP may designate an employee outside of the IT department, provided that the employee is independent of the department using the system for which the logs are being reviewed.

    Note 3: If an IT service provider is utilized on behalf of the LSGP:

        i. If an automated tool is used as discussed in Note 1, notification of issues or errors must be provided to the LSGP.

User Accounts Controls

13. Management personnel, the IT service provider, or persons independent of the department being controlled, establish, or review and approve, user accounts for new employees. Provisioning for user accounts consist of assigning application functions matching the employee's current job responsibilities, unless otherwise authorized by management personnel, to ensure adequate segregation of duties.

14. Provisioning of user accounts for employees who transfer to a new department are performed, or reviewed and approved, by management personnel, or persons independent of the department being controlled. Any previously assigned application function access for the employee's user account is changed to inactive (disabled) prior to the employee accessing their new user account for their role or position in a new department.

INFORMATION TECHNOLOGY

15. When multiple user accounts for one employee per application are used, only one user account may be active (enabled) at a time if the concurrent use of the multiple accounts by the employee could create a segregation of duties deficiency resulting in noncompliance with one or more MICS. Additionally, the user account has a unique prefix/suffix to easily identify the users with multiple user accounts within one application.

16. Locked out user accounts as described in MICS #7(d), may be released by the system after 30 minutes has elapsed. Alternatively, an employee may assist with releasing a locked-out account if the system can produce readily available information which provides reasonable assurance that the user is authorized or through other means as approved. The involvement of an employee assisting in the release of a locked account must be delineated within the written system of internal control .

.

17. The system administrator is notified when an employee/individual is known to be no longer employed or no longer requires user access (e.g., termination of employment or end of service contract). Upon notification, the system administrator changes the status of the user account from active to inactive/disabled status:

    a. Immediately for an employee/individual with remote access;

    b. As soon as possible (not to exceed 48 hours) for a system administrator, IT personnel, or an employee of a service provider; and

    c. Within a reasonable period of time as established by management (not to exceed five days) for all other individuals not described in (a) and (b).

    Note 1: The time period in notifying and changing the status of the user account assumes that it is relatively unlikely the employee/individual will have unauthorized access during that time period.

    Note 2: The written system of internal control delineates the process in notifying the user access administrator and/or system administrator, updating the user account, and the procedures established in preventing the employee/individual from having unauthorized access to the system during that time period.

18. User access listings for gaming applications at the application layer are reviewed quarterly by personnel independent of the authorization and user provisioning processes. The review consists of examining a sample of at least 10% (with a maximum of 25) of the users included in the listing. The reviewer maintains adequate evidence to support the review process, which includes the identified accounts reviewed, documentation of the results of the review, and e-mails or signatures and dates indicating when the user access listing was reviewed. For each of the randomly selected users, determine whether:

    a. The assigned system functions are being used as authorized (i.e., system functions are appropriate for user's job position);

    b. The assigned functions provide an adequate segregation of duties;

c. Terminated employee's user accounts have been changed to inactive (disabled) status within the time period determined by management and delineated within the written system of internal control as required by MICS #17.

Note: Verification of the time period is not required if the system is not capable of providing a user access listing indicating the date and time of an account being disabled/deactivated. The written system of internal control is to delineate this reason for not performing a verification of time period.

d. Passwords have been changed within the last 90 days; and

Note 1: The review for password changes within 90 days applies regardless of whether the system parameter has been configured to have the password changed at least once every 90 days [as required by MICS #7(a)].

Note 2: MICS #18(d) does not apply when the system is not capable of providing a user access listing indicating the date of the last password change. The written system of internal control is to delineate this reason for not performing a review for password changes.

e. There are no inappropriate assigned functions for group membership, if group membership is used in the system.

Note 1: The sample selected for review must be representative of the population. The objective is to include as many different user job positions or group membership profiles as possible.

Note 2: MICS #18(e) applies to a review of the assigned functions for the selected user account with group membership.

Note 3: NOT APPLICABLE

Note 4: The review applies to user access listings for computerized gaming systems with the following capabilities:

i. Generates reports identifying gaming revenues.
ii. Generates statistical gaming records required by the MICS; or
iii. Generates any other records required either by the MICS or by the LSGP's system of internal control.

Generic User Accounts

19. Generic user accounts at the operating system level, if used, are configured such that:

a. The user is automatically brought to the application logon screen immediately upon logging into the operating system, and the user is logged out of the operating system automatically upon exiting the application; or

b. The user is only granted access to the assigned application(s) for the user's current job responsibilities, and the user is precluded from executing unassigned applications or functions from the terminal

desktop and is precluded from interactive access to the operating system through the proper security configurations.

Note: The written system of internal control delineates the method used to secure generic accounts.

20. Generic user accounts at the application level is prohibited unless user access is restricted to inquiry only functions or is specifically allowed in other sections of the MICS.

Service and Default Accounts

21. Service accounts, if used, are utilized in a manner to prevent unauthorized and inappropriate usage to gain logical access to an application and the underlying databases and operating system. The employee responsible for the documentation indicating the method used to prevent unauthorized and inappropriate usage of these service accounts must be delineated within the written system of internal control. The noted documentation must be made available upon request by authorized internal and external auditors and by Lottery personnel.

    Note: Suggested methods include: (1) Service accounts are configured such that the account cannot be used to directly log in to the console of a server or workstation; (2) Service account passwords are to be changed at least once every 90 days, and immediately upon termination of system administrators; (3) Service account login and password information is restricted to a limited number of authorized employees.

22. User accounts created by default (default accounts) upon installation of any operating system, database or application are configured to minimize the possibility that these accounts may be utilized to gain unauthorized access to system resources and data. The employee responsible for the documentation indicating the procedures implemented to restrict access through the use of default accounts must be delineated within the written system of internal control. The noted documentation must be made available upon request by authorized internal and external auditors and by the Lottery.

23. Any other default accounts that are not administrator, service, or guest accounts should be disabled unless they are necessary for proper operation of the system. If these accounts must remain enabled, the passwords are changed at least once every 90 days.

Administrative Access

Note: Administrative access means access that would allow a user to:

i. Add, change, or delete user accounts and associated user provisioning for database, operating system, and network layers
ii. Modify operating system, database, and application security and policy parameters
iii. Add, change, or delete system exception logging information
iv. Add, change, or delete permissions to data files and folders

24. Access to administer the network, operating system, applications, and database security and system parameters is limited to IT personnel under the supervision of supervisory and/or management employees of the LSGP's IT department. If there is no IT department, supervisory or management personnel

independent of the department using such system and/or application may perform the administrative procedures.

25. NOT APPLICABLE.

    Note: NOT APPLICABLE

Backups

26. Daily backup and recovery procedures are in place and, if applicable, include:

    a. Application data.

    Note: This standard only applies if data files have been updated.

    b. Application executable files (unless such files can be reinstalled).

    c. Database contents and transaction logs.

27. Upon completion of the backup process, the backup media is immediately transferred to a location separate from the location housing the servers and data being backed up (for temporary and permanent storage). The storage location is secured to prevent unauthorized access and provides adequate protection to prevent the permanent loss of any data.

    Note: Backup data files and programs can be maintained in a secured manner.

28. Backup system logs, if provided by the system, are reviewed at a Lottery approved cadence by IT personnel or individuals authorized by IT personnel to ensure that backup jobs execute correctly and on schedule. The backup system logs and adequate evidence to support the review process are maintained for the most recent 30 days. The employee(s) responsible for reviewing the backup logs must be delineated within the written system of internal control.

29. The employee responsible for the documentation indicating the procedures implemented for the backup processes and for restoring data and application files must be delineated within the written system of internal control. The noted documentation must be made available upon request by authorized internal and external auditors and by Lottery personnel.

30. IT personnel test a sample of backup recovery procedures, with each system tested at least once annually A record is to be maintained indicating the date a test of the backup recovery procedures was performed and the results of the recovery test.

Recordkeeping

31. A list of all Lottery regulated systems (hardware and software) is maintained which includes the system name, version identifier, , and the related operating system and database, including the applicable hardware and software for each. The list must indicate the period of time each version was in use.

INFORMATION TECHNOLOGY

32. System administrators maintain a current list of all enabled generic, system, and default accounts. The employee(s) responsible for maintaining the list must be delineated within the written system of internal control. The documentation includes, at a minimum, the following:

    a. Name of system (e.g., the application, operating system, or database).

    b. The user account login name.

    c. A description of the account's purpose.

    d. A record (or reference to a record) of the authorization for the account to remain enabled.

    Note: NOT APPLICABLE

33. If an IT service provider is used, the system administrator (the employee(s) delineated within the written system of internal control maintains an additional list of all user accounts with system administrative permission which includes at a minimum:

    a. Name of the system administered by an IT service provider; and

    b. The user account(s) login name(s) used by an IT service provider.

34. The current lists required by MICS #32 and by MICS #33 (if an IT service provider is used) are reviewed by the LSGP in addition to the system administrator, annually. The list required by MICS #32 is reviewed to identify any unauthorized or outdated accounts. The list required by MICS #33 is reviewed to ensure that the permissions are appropriate for each user's position. The written system of internal control is to delineate the employee(s) responsible for the review.

35. User access listings (requirements listed at MICS #10) for all gaming systems are to be reviewed annually.. The lists above may be archived electronically if the listing is written to unalterable media (secured to preclude alteration). If available, the list of users and user access for any given system is in electronic format that can be analyzed by analytical tools (i.e., spreadsheet or database) that may be employed by the Lottery..

    Note: NOT APPLICABLE

36. The IT department maintains current documentation with respect to the network topology (e.g., flowchart/diagram), deployment of servers housing applications and databases, and inventory of software and hardware deployed. The employee responsible for maintaining the current documentation on the network topology must be delineated within the written system of internal control. The noted documentation must be made available upon request by authorized internal and external auditors and the Lottery.

Use of Electronic Signature

37. Procedures for establishing electronic signature functionality are controlled in a manner that precludes any one individual from creating and/or resetting an account or swipe card, setting passwords, pins, or

biometrics, and producing a fraudulent signature. Such procedures must be delineated within the written system of internal control.

38. When an electronic signature is utilized for the completion of a required document or record (e.g., patron or employee) the procedures and controls ensuring authenticity and validity of the signature must be delineated within the written system of internal control include at a minimum:

    a. Description of each signature type used (e.g., electronically stored image capture, electronically signing with stylus, pin, or swipe card).

    b. Description of the authentication process for each signature type, which includes the proper recognition of a user's identity (e.g., patron or employee) in obtaining a valid signature; and

    c. Method used to store the document or record for compliance with MICS #39 and #40.

Electronic Storage of Documentation

Note: Original documents and summary reports may be printed or stored electronically. See MICS #39 and #40 below when stored electronically.

39. When unalterable storage media is used, the documents and summary reports may be scanned or directly stored with the following conditions:

    a. The storage media must contain the exact duplicate of the original document.

    b. All documents stored must be maintained with a detailed index containing the LSGP department and date. This index must be available upon Lottery request.

    c. Upon request by the Lottery , hardware (terminal, printer, etc.) must be provided in order to perform audit procedures.

    d. Controls must exist to ensure the accurate reproduction of records, up to and including the printing of stored documents used for audit purposes.

    e. LSGP personnel must review a sample of the documents on the storage media to ensure the clarity and completeness of the stored document at an approved cadence by the Lottery.

40. When alterable storage media (e.g., off-the-shelf electronic document retention system) is used, procedures which provide at least the same level of control as described by MICS #39 are required. Such procedures must be delineated within the written system of internal control.

    Note 1: For off-the-shelf electronic document retention systems, the controls must include at a minimum, but are not limited to, the configurability to both maintain the version control and limit access to adding or modifying documents, logging all changes, and providing an audit trail of all system administrator activity.

Note 2: If adequate procedures cannot be implemented, the alterable media may not be relied upon for the performance of any audit procedures, and the original documents and summary reports must be retained.

Creation of Wagering Instruments and Wagering Instrument Data Files

Note: MICS #41 - #45 apply when creating wagering instruments within the existing cashless wagering database (creating wagering instruments to distribute to patrons for play at wagering devices) or data files are created to generate instruments to be accepted by the existing cashless wagering system..

41. A Lottery approved system must be utilized when creating wagering instruments to be accepted into the cashless wagering system.

42. NOT APPLICABLE

43. A record is maintained detailing the creation of wagering instruments and/or data files, including evidence of user acceptance, date in service, and personnel involved.

44. NOT APPLICABLE

45. The procedures used and subsequent results relating to the wagering instruments data files review and test are documented and maintained.

Network Security and Data Protection

46. If guest networks are offered (such as, networks that provide internet access for patrons, hotel guests, or vendors), adequate logical segregation is provided of the guest network from the network used to serve access to sports gaming and other devices. Traffic on guest networks is non-routable to the network servicing sports gaming. .

47. Production networks serving LSGP equipment, wagering devices, etc., systems are secured from outside traffic (e.g., firewall or routers) such that systems are configured to detect and report security related events. The employee responsible for the documentation indicating the procedures for detecting and reporting security related events must be delineated within the written system of internal control. The noted documentation must be made available upon request by authorized internal and external auditors and by the Lottery.

    Note: A suggested method in complying with this standard is to configure the system to log unauthorized logins, failed login attempts, and other security related events; and block all unused ports and any in-bound connections originating from outside the network.

48. Network shared drives containing application files and data for all Lottery regulated software, if used, are secured such that only authorized personnel may gain access.

49. All wagering devices (e.g., electronic tablets or other portable terminals), or kiosks are to automatically secure themselves after a reasonable period of inactivity as approved the Lottery. Such devices are secured

to prevent unauthorized access. The methods and procedures, for each type of device, must be delineated within the written system of internal control, and include at a minimum:

a. The reasonable period of inactivity as determined by LSGP and approved by the Lottery.

b. For all wagering devices and kiosks:

i. The system functions and/or applications which are available or can be accessed on or through each device/kiosk;
ii. The controls over user access to the system functions and applications; and
iii. The procedures utilized to secure the network when such devices/kiosks are in use.

c. NOT APPLICABLE

50. Login accounts and passwords required to administer network equipment are secured such that only authorized IT personnel may gain access to these devices. The passwords for these accounts meet the security parameters of IT MICS #7 and are immediately disabled when IT personnel are terminated.

51. Documentation is maintained delineating the policies and procedures established to secure data from unauthorized, accidental exposure, or loss of data due to other mistake or malicious conduct and include controls to prevent, detect, and report such events. The employee responsible for the documentation indicating the procedures for preventing, detecting, and reporting data exfiltration events must be delineated within the written system of internal control The noted documentation must be made available upon request by authorized internal and external auditors and by the Lottery.

Note: Unauthorized accidental disclosure, exposure, or loss of sensitive data can occur due to an accidental or deliberate move from inside an organization to outside an organization without permission. This includes the use of technology (e.g., data moved via use of file share, cloud system, external memory device, or mobile device) or any other means (e.g., malware or social engineering) to steal sensitive data.

52. Documentation is maintained delineating the policies and procedures established to protect systems, networks, programs, devices, and data from unauthorized access or use and ensuring integrity, confidentiality, and availability of information. The employee responsible for the documentation indicating the policies and procedures implemented must be delineated within the written system of internal control. The noted documentation must be made available upon request by authorized internal and external auditors and by the Lottery.

53. Documentation is maintained delineating the policies and procedures established to protect a patron's personally identifiable information, including, but not limited to:

Note 1: "Personally identifiable information" means any information about an individual maintained by a LSGP including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Note 2: The employee responsible for this documentation required by this standard must be delineated within the written system of internal control. The noted documentation must be made available upon request by authorized internal and external auditors and by Lottery personnel.

a. The designation and identification of one or more management officials having primary responsibility for the design, implementation and ongoing evaluation of such procedures and controls;

b. The procedures to be used to determine the nature and scope of all personally identifiable information collected, the locations in which such information is stored, and the devices or media on which such information may be recorded for purposes of storage or transfer;

c. The procedures to be used to prohibit access to a patron's unique personal identification number ("password").

d. The procedures to be used to reasonably ensure only a patron will be changing its password as the holder of an account;

e. The policies to be utilized to protect personally identifiable information from unauthorized access by employees, business partners, and persons unaffiliated with the company;

f. Notification to a patron of privacy policies;

g. Procedures to be used in the event the operator determines that a breach of data security has occurred, including required notification to the Lottery and

h. Provision for compliance with all local, state and federal laws concerning privacy and security of personally identifiable information.

54. The cybersecurity risk assessment and/or cyber-attack reports, along with any supporting documentation, is to be made available upon request by authorized internal and external auditors and by Lottery personnel.

Remote Access

55. For each LSGP system application that can be accessed remotely for purposes of obtaining vendor support, the written system of internal control must specifically address remote access procedures including, at a minimum:

a. Type of system, vendor's name and business address (business address only for cashless wagering systems), and version number, if applicable.

b. The method and procedures used in establishing and using passwords to allow authorized vendor personnel to access the system through remote access.

c. The personnel involved, and procedures performed to enable the method of establishing remote access connection to the system when the vendor requires access to the system through remote access.

d. The personnel involved, and procedures performed to ensure the method of establishing remote access connection is disabled when the remote access is not in use.

e. Any additional requirements relating to remote access published by the Lottery.

56. In the event of remote access, prepare a complete record of the access to include:

a. Name or identifier of the LSGP's employee authorizing access;

b. Name of manufacturer/vendor;

c. Name or identifier of manufacturer's/vendor's employee accessing system;

d. Name of user account(s) through which the vendor's employee accessed the system;

e. Name of system(s) accessed by the vendor;

f. Adequate and detailed description of work performed (including the old and new version numbers of any software that was modified); and

g. Date, time, and duration of access.

57. User accounts used by vendors must remain disabled on all operating systems, databases, network devices, and applications until needed by such vendor. Subsequent to an authorized use by a vendor, the account is returned to a disabled state.

58. Remote access for all vendors is enabled only when approved by authorized IT personnel.

59. If remote access to the production network (live network) is available and allows access to sports gaming applications, such access is logged automatically by the device or software where it is established, if the system is capable of automatically logging such access. If automated logging is available, the log is to indicate the date/time of such access and the identification of the individual/user account (e.g., vendor or employee) performing access.

Note: The written system of internal control is to delineate whether automated logging is performed and the device or software performing this function.

Changes to Production Environment

60. Documentation is maintained delineating a comprehensive and robust change control process to prevent any unauthorized changes being incorporated into the production environment. The employee responsible for the documentation of the change control process must be delineated within the written system of internal control. The noted documentation must be made available upon request by authorized internal and external auditors and by the Lottery . The documented process includes at a minimum:

a. Proposed changes to the production environment are evaluated sufficiently by management personnel prior to implementation;

b. Proposed changes are properly and sufficiently tested prior to implementation into the production environment;

c. A strategy of reverting back to the last implementation is used (rollback plan) if the install is unsuccessful and the rollback plan is tested prior to implementation to the production environment; and

d. Sufficient documentation is maintained evidencing management approvals, testing procedures and results, rollback plans, and any issues/resolutions encountered during implementation.

Note: The above process includes all changes to the production environment (operating system, network, databases, and applications) that relate to critical IT systems, and sports gaming systems.

Information Technology Department

Note: If a separate IT department is maintained or if there are in-house developed systems, MICS #61 through #64 are applicable. The IT department may consist of the LSGP's IT personnel or an IT service provider.

61. The IT department is independent of all gaming departments.

62. IT personnel are precluded access to wagering instruments and gaming related forms.

In-House Software Development

63. If source code for gaming systems is developed or modified internally, a process is adopted to manage the development. The employee responsible for the documentation indicating the process in managing the development or modification of source code must be delineated within the written system of internal control. The noted documentation must be made available upon request by authorized internal and external auditors and by the Lottery. The process must address, at a minimum:

    a. Requests for new programs or program changes are reviewed by the IT supervisory personnel. Approvals to begin work on the program are documented.

    b. A written plan of implementation for new and modified programs is maintained and includes, at a minimum, the date the program is to be placed into service, the nature of the change (if applicable), a description of procedures required in order to bring the new or modified program into service (conversion or input of data, installation procedures, etc.), and an indication of who is to perform all such procedures.

    c. Sufficiently documenting software development and testing procedures.

    d. Documentation of approvals, development, testing, results of testing, and implementation into production. Documentation includes a record of the final program or program changes, including evidence of user acceptance, date in service, programmer, and reason for changes, is documented and maintained.

e. Physical and logical segregation of the development and testing from the production environments.

f. Adequate segregation of duties (i.e., those who develop/test code do not have access to introduce new or modified code into the production environment).

Note: For MICS #63(e) and (f) a system administrator is precluded from developing/testing code which will be introduced into the production environment.

g. Secured repositories for maintaining code history.

h. End-user documentation (guides and manuals).

64. NOT APPLICABLE

Purchased Software Programs

Note: IT MICS #65 applies when IT personnel perform in-house modifications to a purchased software program.

65. New programs and program changes for purchased systems are documented as follows:

a. Documentation is maintained and includes, at a minimum, the date the program was placed into service, the nature of the change, a description of procedures required in order to bring the new or modified program into service (conversion or input of data, installation procedures, etc.), and an indication of who performed all such procedures.

b. A copy of the associated equipment reporting form submitted to the Lottery for each new program or program change, and a record that such software was approved for use, is maintained.

c. Testing of new and modified programs is performed (by the LSGP or the system manufacturer) and documented prior to full implementation.

Data Access Control

Note: MICS #66 through #68 apply to any Lottery approved LSGP gaming systems including systems utilizing promotional accounts and/or wagering accounts. The written system of internal control is to delineate the methods and procedures in Ohio rule ORC 3775-16-15 – OAC 3770: 3-6-02.

66. Procedures are in place to ensure that no alteration is permitted of any system stored transaction history or event log information that was properly communicated from the game, gaming device or generated by the application.

67. Procedures are in place to ensure that all critical system stored data are non-alterable other than through normal operation processes. Critical system data includes data relating to, but not limited to, validation numbers and dollar value of wagering instruments, personal identification numbers and account balances of promotional and wagering accounts, and unpaid winning ticket information.

INFORMATION TECHNOLOGY

Note: Methods may include, but are not limited to, checksums on data tables or database encryption.

68. Procedures are in place to ensure that any communication with equipment or programs external to the approved system is performed through a Lottery approved secure interface. The documentation evidencing approval is maintained and available upon request.

    Note: Documentation may include, but is not limited to, detailed network topology diagrams indicating all interfaces utilized to access Lottery approved systems by external programs.