Proposed Revisions Resulting from Industry Comments
Draft MICS V9 Dated 10/24/2022

Section/ MICS #	MICS Quote	GCB's Revised MICS
Cage and Credit MICS #12	12. The voiding process for cage markers is completed no later than 30 minutes after the issuance of the marker unless the reason for exceeding this time period is documented on one part of the marker or other document (e.g., a log) sufficiently identifying the marker. Note: The reason for exceeding the 30 minute time period is to be separately documented from the reason the marker is voided.	***MICS Revised:*** 12. The voiding process for cage markers is completed no later than 30 minutes after the issuance of the marker unless the reason for exceeding this time period is documented on one part of the marker or other document (e.g., a log) sufficiently identifying the marker. Note: The reason for exceeding the 30 minute time period is to be ~~separately~~ documented ~~from~~ *in addition to* the reason the marker is voided.
Entertainment MICS #32		***MICS Added:*** *32. Prior to submission of the NGC tax returns for the month, the reconciliation required by MICS #31 is completed, and any follow-up performed is documented and maintained. Any variances noted are resolved prior to submission of the tax returns.*
Information Technology MICS #3	3. Procedures are in place to ensure the oversight by licensee 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 pursuant to Regulation 6.090 and available upon request. Note: Procedures may include, but are not limited to, changes made to the systems or notification of security incidents.	***MICS Revised:*** 3. *Documentation is maintained delineating the policies and* procedures ~~are in place~~ *established* to ensure the oversight by licensee 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 pursuant to Regulation 6.090. ~~and available upon request.~~ *The noted documentation must be made available upon request by authorized internal and external auditors and by Board personnel.* Note: Procedures may include, but are not limited to, changes made to the systems or notification of security incidents.
Information Technology Note before MICS #4	***Physical Access and Maintenance Controls*** 4. The critical IT systems and equipment for each gaming application (e.g., keno, race and sports, slots, or cashless wagering systems) and each application for entertainment are maintained in a secured area (secured area includes a hosting center). The area housing the critical IT systems and equipment for each gaming and entertainment application and other critical IT systems and equipment are equipped with the following:	***MICS Note Added:*** ***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 gaming application (e.g., keno, race and sports, slots, or cashless wagering systems) and each application for entertainment are maintained in a secured area (secured area includes a hosting center). The area housing the critical IT systems and equipment for each gaming and entertainment application and other critical IT systems and equipment are equipped with the following:

Proposed Revisions Resulting from Industry Comments
Draft MICS V9 Dated 10/24/2022

Section/ MICS #	**MICS Quote**	**GCB's Revised MICS**
	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 slot gaming 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 and equipment for gaming and entertainment applications. c. The administration of the electronic security systems, if used to secure areas housing gaming and entertainment critical IT systems and equipment, is performed by personnel independent of a gaming or entertainment department. Note: The written system of internal control pursuant to Regulation 6.090 is to delineate the methods, processes and practices used in meeting the requirements of MICS #4 (a through c).	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 slot gaming 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 and equipment for gaming and entertainment applications. c. The administration of the electronic security systems, if used to secure areas housing gaming and entertainment critical IT systems and equipment, is performed by personnel independent of a gaming or entertainment department. Note: The written system of internal control pursuant to Regulation 6.090 is to delineate the methods, processes and practices used in meeting the requirements of MICS #4 (a through c).
Information Technology MICS #5	5. Access to areas housing critical IT systems and equipment for gaming and entertainment applications, including vendor supported systems, is restricted to authorized IT personnel. Gaming and entertainment department personnel, including the manufacturers of the gaming and entertainment computer equipment, are only allowed access to the areas housing critical IT systems and equipment for gaming and entertainment applications, including vendor supported systems, when authorized by IT personnel and with periodic monitoring by IT personnel during each access.	***MICS Revised:*** 5. Access to areas housing critical IT systems and equipment for gaming and entertainment applications~~, including vendor supported systems,~~ is restricted to authorized IT personnel. Gaming and entertainment department personnel, including the manufacturers of the gaming and entertainment computer equipment, are only allowed access to the areas housing critical IT systems and equipment for gaming and entertainment applications~~, including vendor supported systems,~~ when authorized by IT personnel and with periodic monitoring by IT personnel during each access.
Information Technology MICS #6	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	***MICS Revised:*** 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

Proposed Revisions Resulting from Industry Comments
Draft MICS V9 Dated 10/24/2022

Section/ MICS #	MICS Quote	GCB's Revised MICS
	e. The name of IT personnel authorizing such access.	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 MICS #16	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. The involvement of an employee assisting in the release of a locked account must be delineated within the written system of internal control pursuant to Regulation 6.090.	***MICS Revised:*** 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 approved by the Board*. The involvement of an employee assisting in the release of a locked account must be delineated within the written system of internal control pursuant to Regulation 6.090.
Information Technology MICS #18	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 employees 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	***MICS Revised:*** 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 employees 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

Section/ MICS #	MICS Quote	GCB's Revised MICS
	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 positions so that each user position is reviewed at least annually. If a group membership is used, ensure that each group is represented in the sample and reviewed at least annually. Note 2: MICS #18(e) applies to a review of the assigned functions for the selected user account with group membership. Note 3: The required review of user access listings does not apply to user access listings for any entertainment tax related applications. Note 4: The review applies to user access listings for computerized gaming systems with the following capabilities: • Generates reports identifying gaming revenues; • Generates detailed records of all markers, IOU's, returned checks, hold checks, or other similar credit instruments; • Generates statistical gaming records required by the MICS; or • Generates any other records required either by the MICS or by the licensee's system of internal control.	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. ~~so that each user position is reviewed at least annually. If a group membership is used, ensure that each group is represented in the sample and reviewed at least annually.~~ Note 2: MICS #18(e) applies to a review of the assigned functions for the selected user account with group membership. Note 3: The required review of user access listings does not apply to user access listings for any entertainment tax related applications. Note 4: The review applies to user access listings for computerized gaming systems with the following capabilities: • Generates reports identifying gaming revenues; • Generates detailed records of all markers, IOU's, returned checks, hold checks, or other similar credit instruments; • Generates statistical gaming records required by the MICS; or • Generates any other records required either by the MICS or by the licensee's system of internal control.
Information Technology MICS #26	26. Daily backup and recovery procedures are in place and, if applicable, include:	***MICS Revised – Note Added Back In:*** 26. Daily backup and recovery procedures are in place and, if applicable, include:

Section/ MICS #	MICS Quote	GCB's Revised MICS
	a. Application data. b. Application executable files (unless such files can be reinstalled). c. Database contents and transaction logs.	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.
Information Technology MICS #51	51. Procedures are in place 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 pursuant to Regulation 6.090. The noted documentation must be made available upon request by authorized internal and external auditors and by Board personnel. 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.	***MICS Revised:*** 51. *Documentation is maintained delineating the policies and* procedures ~~are in place~~ *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 pursuant to Regulation 6.090. The noted documentation must be made available upon request by authorized internal and external auditors and by Board personnel. 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.
Interactive Gaming MICS #41	41. "User Access Listing" reports produced 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 selected user accounts reviewed, documentation of the results of the review, and e-mails or signatures and dates indicating the individual(s) performing the review and 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;	***MICS Revised:*** 41. "User Access Listing" reports produced 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 selected user accounts reviewed, documentation of the results of the review, and e-mails or signatures and dates indicating the individual(s) performing the review and 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;

Proposed Revisions Resulting from Industry Comments
Draft MICS V9 Dated 10/24/2022

Section/ MICS #	MICS Quote	GCB's Revised MICS
	c. Terminated employees' user accounts have been changed to inactive (disabled) status; d. Passwords have been changed within the last 90 days; and Note: 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. e. There are no inappropriate assigned functions for group membership, if applicable. Note 1: MICS #41(e) applies to a review of the assigned functions for the selected user account with group membership. Note 2: The sample selected for review must be representative of the population. The objective is to include as many different user positions so that each user position is reviewed at least annually. If a group membership is used, ensure that each group is represented in the sample and reviewed at least annually.	c. Terminated employees' user accounts have been changed to inactive (disabled) status; d. Passwords have been changed within the last 90 days; and Note: 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. e. There are no inappropriate assigned functions for group membership, if applicable. Note 1: MICS #41(e) applies to a review of the assigned functions for the selected user account with group membership. Note 2: 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. ~~so that each user position is reviewed at least annually. If a group membership is used, ensure that each group is represented in the sample and reviewed at least annually.~~
Slots MICS #64	64. Payouts recorded on a manual payout form, including jackpots, fills, cancelled credits, short pays exceeding $10 and promotional payouts exceeding $100 that are deducted from gross gaming revenue, are controlled and completed in a manner that precludes a custodian of funds from altering the dollar amount on all parts of the payout form subsequent to the payout and misappropriating the funds.	***MICS Revised:*** 64. Payouts recorded on a manual payout form, including jackpots, fills, cancelled credits, short pays exceeding $~~10~~*20* and promotional payouts exceeding $100 that are deducted from gross gaming revenue, are controlled and completed in a manner that precludes a custodian of funds from altering the dollar amount on all parts of the payout form subsequent to the payout and misappropriating the funds.
Table Games MICS #16	16. The voiding process is completed no later than 30 minutes after the issuance of the marker unless the reason for exceeding this time period is documented on one part of the marker or other document (e.g., a log) sufficiently identifying the marker. Note: The reason for exceeding the 30 minute time period is to be separately documented from the reason the marker is voided.	***MICS Revised:*** 16. The voiding process is completed no later than 30 minutes after the issuance of the marker unless the reason for exceeding this time period is documented on one part of the marker or other document (e.g., a log) sufficiently identifying the marker. Note: The reason for exceeding the 30 minute time period is to be ~~separately~~ documented ~~from~~ *in addition to* the reason the marker is voided.