



HORSESHOE COUNCIL BLUFFS

SPORTSBOOK

INTERNAL CONTROL STANDARDS

Note: The following Sports Internal Control Standards pertain William Hill US, hereinafter collectively referred to as “WHUS”.

Contents

Definitions	3
Equipment Standards and Record Keeping	4
House Rules.....	6
Wagering Standards.....	6
Book Wagering Reports	7
Payout Standards	7
Betting Kiosks	8
Wagering Accounts	8
Promotional Contests, Tournaments, Drawings and Giveaway Programs	13
Checkout Standards	15
Employee Segregation of Duties	16
Generic Passwords for Casino Cage Cashiers	18
Computerized Player Tracking Systems.....	18
Computer Reports.....	19
Accounting/Audit Standards	23
Payout Procedures for Mail-In Winning Sports Tickets and Vouchers	27
Prohibited Patrons	27
Self-Exclusion	28
Offset Program Requirement.....	30
Global Risk Management.....	30
Annual Audit Requirement.....	30
Information Technology Controls	30
Definitions	30
Physical Access and Maintenance Controls	32
System Parameters	33
User Accounts	37
Generic User Accounts.....	39
Service & Default Accounts	40
Administrative Access.....	40
Backups	41
Recordkeeping.....	42
Electronic Storage of Documentation	43
Network Security and Data Protection	43
Remote Access	44
Changes to Production Environment.....	45

Information Technology Department	46
In-House Software Development	46
Purchased Software Programs	47
Data Access Control	47
Independent Laboratory Testing.....	49

Note 1: The term “voucher” as used in these ICS refers to a printed wagering instrument, usually issued for use in a betting kiosk, with a fixed dollar wagering value and is redeemable for cash or cash equivalents. Unredeemed vouchers that are issued as payment for winning wagers are included in revenue when the vouchers expire (i.e., purged vouchers are included in gross revenue).

Note 2: The term “betting kiosk” as used in these ICS refers to a self-activated machine that patrons use to place wagers, open accounts, make account deposits and/or withdrawals (withdrawals are not currently permitted at WHUS kiosks) and is considered a writer/cashier station. ICS applicable to writers/cashiers (or writer/cashier stations) are also applicable to a betting kiosk unless otherwise stated within the ICS.

Note 3: A “signature” on a document provides evidence of the person’s involvement and/or authorization of the intentions reflected in this document. It is typically in the form of a stylized script associated with a person. The stylized script “signature” may include the first letter of the person’s first name along with the person’s full last name.

Note 4: If the sports department utilize wagering accounts and is the designated area of accountability, compliance with cage and credit ICS for wagering accounts is required. Such procedures are delineated within the written system of internal controls.

Note 5: If wagering accounts are limited to sports books only, then, verification of a patron’s identification may be performed at central site books or affiliated book.

Definitions

“Administrator” means the administrator of the Iowa racing and gaming commission or the administrator’s designee.

“Adjusted gross receipts” means the gross receipts less winnings paid to wagerers on gambling games. However, it does not include promotional play receipts received after the date in any fiscal year that the commission determines that the wagering tax imposed pursuant to Iowa code section 99F.11 on all licensees in that fiscal year on promotional play receipts exceeds twenty-five million eight hundred twenty thousand dollars.

"Advance deposit sports wagering" means a method of sports wagering in which an eligible individual may, in an account established with a licensee under Iowa Code section 99F.7A, deposit moneys into the account and use the account balance to pay for sports wagering. Prior to January 1, 2021, an account must be established by an eligible individual in person with a

licensee.

"Advance deposit sports wagering operator" means an advance deposit sports wagering operator licensed by the commission who has entered into an agreement with a licensee under Iowa Code section 99F.7A to provide advance deposit sports wagering.

"Authorized sporting event" means a professional sporting event, collegiate sporting event, international sporting event, or professional motor race event. "Authorized sporting event" does not include a race as defined in Iowa Code section 99D.2, a fantasy sports contest as defined in Iowa Code section 99E.1, minor league sporting event, or any athletic event or competition of an interscholastic sport as defined in Iowa Code section 9A.102.

"Collegiate sporting event" means an athletic event or competition of an intercollegiate sport as defined in Iowa Code section 9A.102.

"Commission" means the racing and gaming commission created under Iowa Code section 99D.5.

"Designated sports wagering area" means an area, as designated by a licensee and approved by the commission, in which sports wagering is conducted.

"Eligible individual" means an individual who is at least twenty-one years of age or older who is located within this state.

"Facility" means an entity licensed by the commission to conduct pari-mutuel wagering, gaming or sports wagering operations in Iowa.

"International sporting event" means an international team or individual sporting event governed by an international sports federation or sport's governing body including, but not limited to, sporting events governed by the international Olympic committee and the international federation of association football.

"Licensee" means any person licensed under Iowa Code section 99F.7 or 99F.7A.

"Minor league sporting event" means a sporting event conducted by a sports league which is not regarded as the premier league in the sport as determined by the commission.

"Professional sporting event" means an event, excluding a minor league sporting event, at which two or more persons participate in sports or athletic events and receive compensation in excess of actual expenses for their participation in such event.

"Sports wagering" means the acceptance of wagers on an authorized sporting event by any system of wagering as authorized by the commission. Sports wagering does not include placing a wager on the performance or nonperformance of any individual athlete participating in a single game or match of a collegiate sporting event in which a collegiate team from this state is a participant or placing a wager on the performance of athletes in an individual international sporting event governed by the international Olympic committee in which any participant in the international sporting event is under eighteen years of age.

"Sports wagering net receipts" means the gross receipts less winnings paid to wagerers on sports wagering.

Equipment Standards and Record Keeping

1. The Writer must examine and test the stamping machine, daily, to ensure the date is correct and the time is to the nearest minute. The test results must be kept at each location. The date/time stamping machines used for voided tickets and manual payouts have a backup battery installed as a power supply in the event of power loss to the machines.

2. The Writer must document the results of the test in a log, which includes the station number, date, time of test, time per computer, name or signature of employee performing the test, and any other relevant information. Writers do not have access to adjust the clock. Adjustments to clocks are made by Book Supervisors or the Book Manager, and those adjustments are recorded on the log.
3. The date and time generated by the CBS computer system time is tested daily by a member of Customer Support, who is independent of the book and does not have cashiering capabilities, located at WHUS' Sunset Office, 8329 W Sunset Rd. #100, Las Vegas, NV 89118. This testing for each satellite book is performed at the satellite location.
4. The Customer Support Department contacts the Naval Observatory Master Clock daily to verify that the CBS time is correct. If the time is incorrect, the Software Support Department is contacted to adjust the time. A log is maintained for each verified recording of the time of the Master Clock, CBS Clock, time difference (if any), initials of the employee performing verification, issues and resolutions.
5. Initial testing- All equipment and systems integral to the conduct of sports wagering and advance sports wagering shall be tested and certified for compliance with commission rules and the standards required by the commission designated independent testing laboratory. Certification and commission approval must be received prior to using any equipment or system to conduct sports wagering.
6. Change control- The licensees and advance deposit sports wagering operators shall submit change control processes that detail evolution procedures for all updates and changes to equipment and systems to administer for approval. These processes shall include details for identifying critically for updates and determining of submission of updates to an independent testing laboratory for review and certification.
7. Annual testing- a system integrity and security risk assessment shall be performed annually on sports wagering and advance deposit sports wagering system.
 - The testing organization must be independent of the license and shall be qualified by the administrator
 - The system integrity and security risk assessment shall be conducted no later than 90 days after the start of the licensee's fiscal year.
 - Results from the risk assessment shall be submitted to the administrator no later than 30 days after the assessment is conducted.
 - At the discretion of the administrator, additional assessments or specific testing criteria may be required.
8. WHUS shall maintain adequate records of the business operations which shall include:
 - All correspondence with the administrator and other governmental agencies on the local, state and federal level
 - All correspondence between WHUS and any of its customers who are applicants or licensees under the Iowa Code chapter 99F.
 - A personnel file on each employee of WHUS, including sales representatives.
 - Financial records of all transactions with facilities

House Rules

Pursuant to Iowa Administrative rule 13.2(4) Submitted and approved House Rules for WHUS will be prominently displayed in the sports wagering area, available for review on all available media platforms (Kiosks, Mobile Application and at the sportsbook window) as well as in the Terms and Conditions/Terms of Service accepted by patrons when a wagering account is created.

Wagering Standards

9. Whenever a betting station is opened/closed for wagering or turned over to a new Writer, the Writer signs on/off and the computer documents the Writer's identity, the date and time, the window number, and the fact that the station was opened/closed.

10. When the Writer accepts a wager, a betting ticket is created in duplicate as follows:

- a. An original issued through a printer and given to the customer.

Note: If a wager is placed using communications technology, an original betting ticket does not need to be created.

- b. A restricted computer record, which is generated at the same time as the original ticket. The record contains the ticket number, date and time, and terms of the wager. The terms of the wager include the event/racing meet, number and date, wager selection, type of wager and dollar amount wagered. Sports Book employees are prohibited access to the restricted copy, which is profile controlled by the computer system.

11. When a Writer voids a betting ticket the following procedure will be followed:

- a. A void designation is immediately branded by the computer on the ticket, after a Supervisor or Trader enters their User ID and Password to approve the void. Alternatively, a ticket can be voided manually in the computer system by inputting the ticket sequence number and having a Supervisor or Trader enter their User ID and Password. The Writer then writes 'void' on the original and utilizes the timestamp machine to show the accurate date and time of void.
 - b. For not-in-computer voids, the date and time at which the ticket was voided is stamped on the original.
 - c. All voids are signed by the Writer and a Supervisor, or remotely authorized by a Trader, who did not write the ticket, at the time of the void.

Note: If the original ticket is unavailable (e.g., printer malfunction) a receipt for the void is printed to reflect the void transaction.

12. The cutoff time for event wagering will be set up in the computer system.

13. The computer is incapable of accepting a wager subsequent to the above cutoff times. If the start time of an event has to be extended because of weather or other problems that would prevent an event from starting on time, a report is produced identifying such wagers due to the extension.
14. The computer cannot void a ticket after the cutoff time.
15. The computer cannot change a cutoff time to a time that is earlier than the current time of day.
16. Tickets are not written or voided after the outcome of an event is known.

Book Wagering Reports

17. Within 24-hours after the end of a designated 24-hour period, Multiple Transaction Logs created are submitted to the Compliance Department.

Payout Standards

18. Vouchers issued by the CBS system (including betting kiosks) include the voucher number, the individual book's name and address, the date/time, and the dollar amount of the voucher.

Note: The above ICS applies to vouchers issued as payment for winning wagers, "change due" from a wager transaction and, as a result of a purchase of a voucher.

19. Before a customer can be paid on a winning ticket, results are input into the computer's administrative terminal for computerized grading of all wagers for all systems used. Unpaid winning tickets and voucher reports are restricted to authorized personnel independent of the sports books.
20. Prior to making a payment on a ticket/voucher or crediting the winnings to the customer's wagering account:
 - a. The writer/cashier enters or scans the ticket/voucher number into the CBS computer system to authorize the payment; or
 - b. For wagering account wagers, when the event results are posted in the CBS system, and the CBS system automatically authorizes payment of winnings and updates the customer's wagering account.
21. Upon computer authorization of payment, the computer immediately brands the customer's copy with the amount of payment, date, time and window number. If the computer does not brand the customer's copy, the Writer will staple a printed receipt of the payment to the original ticket.

Note: Any manually paid tickets that had been previously purged from the sports computer system do not need to be entered into the sports computer system. This note does not apply to WHUS.

22. The CBS computer cannot authorize payment on a ticket that has been previously paid, a voided ticket, a losing ticket, a locked ticket or an unissued ticket/voucher.

23. If a progressive pool is used for wagers, copies of the rules are retained.

Betting Kiosks

24. WHUS has established procedures for in-person wagering account registration at a betting kiosk for sports. Such procedures are delineated below.

Wagering Accounts

Wagering Account: Eligibility

Wagering Account Set-up:

1. Customer downloads the application iOS or Android mobile application and navigates to the Account Registration option on the main launch page.
2. Customer enters:
 - a. Email address.
 - b. Phone number.
 - c. Password.
 - d. Last 4 of SSN.

NOTE 1: On the mobile app log in screen there is a link for Forgotten Username and a separate one for Forgotten Password. The Forgotten Username links to Phone chat or Live Chat with Customer Support where an agent can provide the Username based on the customer answering security questions previously set up by the patron. The Forgotten Password link will trigger the emailing of an authentication code to the email address on file. Using the account number and authentication code, the user can reset their password.

NOTE 2: An email notification is sent to the email address on file when any deposit or withdrawal request is made or for any change to registration information (Name, address, phone number, email address),

3. Customer then acknowledges receipt of our Terms of Service, Privacy Policy and that they are not part of the prohibited person's list (i.e. coaches, athletic trainers, officials, etc.).
4. Customer is then requested to scan his or her driver's license or ID, using the mobile phone camera.
5. After scanning the driver's license information, customer can review the information obtained and can make changes to name or address if necessary.
6. The application then validates the format of the above data, and the mobile application stores the information obtained in steps 2 to 5.
7. The current GPS location is transmitted to a back-end REST API that returns addresses of the nearest William Hill licensed sports books (ordered closest first). The sports books addresses are displayed with a message to the customer to complete the registration at a William Hill licensed sports book.
8. Once the customer is physically within a William Hill licensed sports book, they are able to

complete the registration process:

- a. The customer clicks the “I’m Here” button and the mobile application confirms their location. Geo-location is validated using both device GPS and Bluetooth beacons which are physical devices installed at the sports book. The beacons emit a secure wireless signal which is interpreted by the mobile application.
 - b. The customer is requested to take a selfie picture using the mobile device camera.
 - c. The complete registration data are sent over HTTPS to a back-end REST API service. The image(s) are base64 encoded.
 - d. The back-end registration REST API sends the image(s) and its metadata to another REST API that stores the image(s) and metadata. It then places the new registration on a queue (with the social security number and password encrypted)
 - e. The back-end registration service checks the submitted data against the Iowa Self-Exclusion log to verify that the patron is not an excluded person before creating the account.
9. If there is a positive match the patron will receive, and error message and the account creation is ended. The message that is populated is “We are unable to process your application due to the Iowa Self-Exclusion Program”. If you feel this exclusion is an error you can contact Customer Service team at support@williamhill.us or (855) 754-1200, as well as contact Iowa Racing and Gaming Commission for details.
 10. The mobile application informs the customer that the registration is being processed.
 11. Customer data is securely transmitted to a third-party KYC provider (“LexisNexis”) and validated for accuracy for legal name, age and address.
 - a. If the data is validated, a message is sent back to a REST API indicating that the match was successful.
 - b. If the data was not able to be validated, a message is sent back to a REST API indicating that a match could not be validated.
 12. If the KYC validation was successful, the registration process creates a new record within the Sports Betting Platform and customer is notified that their account creation was successful.
 13. If the KYC validation process was not successful, the customer is notified to contact Customer Service who will be able to mitigate the issue and complete the registration process using a Back-Office Portal tool.
 14. WHUS Mobile Application contains William Hill geolocation logic that is employed at login, during bet placement and continually while logged in. This logic verifies that the customer is within the Iowa state boundaries.
 15. Paper applications for wagering accounts will be available at any window within the Sportsbook for patrons to manually create an account.
 16. The customer data is approved or rejected by a Customer Support representative, who verifies that the possible patron is not included on the IRGC Self Exclude Listing (Iowa Code 99F.4(22)).
 17. When the registration is approved by a Customer Support representative then the CBS server creates the account and updates the registration status, via REST API. The mobile application will inform the customer that the registration process is complete and automatically logs the customer into the application.
 18. WHUS limits the number of active accounts per patron to 1 by verifying that the SSN provided is not currently attached to any other account within the wagering system.
 19. Account Lock Up is triggered after 3 failed attempts to access the patrons account. An

authorization code is then emailed to the email address attached to the patrons account. The patron then uses their account number and the authorization code to unlock their account.

20. Patrons can easily set a Daily, Weekly and Monthly deposit limit, there is no specific amount however, the monthly cannot be less than the weekly and the weekly cannot be less than the daily. They can also set a Daily, Weekly and Monthly spend limit within the mobile application. Decreases to the limit are effect immediately. Increases do not take effect for 24 hours to daily limits, 7 days for weekly limits and 30 days for monthly limits. There is no cost associated with setting limits.
21. Furthermore, customers can opt into a time management system that allows you to limit your daily time on our site. After exceeding this period, you will be prevented from further play. All requests for time limit decreases (i.e. going from playing 10 hours a day to 1 hour a day) will be implemented immediately; requests for time limit increases (i.e. going from playing 1 hour a day to unlimited play) only become valid after 30 days.
22. William Hill customers can temporarily suspend their account or self-exclude from further gaming if they have developed gambling-related problems or feel at risk of developing gambling-related problems. You can temporarily suspend your account for any period from 3 to 180 days. Self-exclusion will ban you from all Iowa licensed gaming offered by William Hill Sportsbook for a duration of 1 or 5 years and cannot be revoked. Any person requesting temporary suspension or placement on the Internet self-exclusion list shall submit his or her request through their Internet gaming account. Once your account is created, log in and go to My Account and select the “Responsible Gaming” option. A permanent self-exclusion can be filed in person at the retail counter or calling customer support. There is no cost associated with setting limits

Wagering Account Deposits – Writer

The following delineate the deposit procedures for a WHUS Wagering Account with a Writer:

1. Customer will provide the Writer with their wagering account number.
2. Customer will provide ID to the Writer for verification of identity.
3. Customer will then provide the Writer with the amount of funds to deposit into their wagering account.
4. The Writer processes the deposit in the Teller Terminal.
5. The Teller Terminal produces two tickets. One is signed by the customer and Writer and is placed in the Writer’s audit paperwork. The second is the receipt provided to the customer.

Wagering Account Deposits – Kiosk

The following delineate the deposit procedures for a WHUS Wagering Account at a Kiosk:

1. Customer will enter their WHUS account number into the Kiosk.
2. Customer enters a personal identification number (PIN).

3. The account is verified, and the customer may now deposit funds into the account by means of a bill acceptor incorporated within the Kiosk.
4. The Kiosk prints a receipt confirming the deposit into the WHUS account. The receipt will include the customer's WHUS account identification number, name and deposit amount.

Wagering Account Deposits – Pre-paid Card

The following delineate the deposit procedures for a William Hill US (WHUS) Wagering Account utilizing the William Hill Priority Access Pre-Paid Card

1. A Customer desiring to deposit into a WHUS wagering account may initiate the William Hill Priority Access Pre-Paid Card deposit request using their mobile device.
2. The customer will launch the WHUS Mobile Client and log into their account using their personal identification number (PIN).
3. Once the account is verified, the customer may choose the deposit funds option.
4. The amount of the deposit is selected.
5. The deposit window opens, and the customer chooses the William Hill Priority Access Pre-Paid Card (WHPAC) payment method.
6. Customer transfer funds from the WHPAC into the William Hill Sports wagering account.
7. For new Payments customers:
 - a. Customer is presented with the "Add Deposit Method Screen."
 - b. Customer completes the debit card information form and taken to the finalize deposit screen
 - c. Customer reviews/approves card and deposit details. Moves onto enrollment screen.
 - d. Customer completes William Hill Priority Access enrollment screen.
 - e. Upon completion of enrollment the customer is taken to the transfer screen.

Upon completion of registration and authentication, the patron can deposit funds into their William Hill sports book account.

A patron's Internet gaming account may be funded using:

- Debit card
- ACH/e-check
- William Hill Prepaid Card
- Cash funding at William Hill retail sports book

All deposits will be made available to the patron for gambling immediately upon successful authorization.

All patron deposits are monitored for overall transaction amount. Please see the tables (In Appendices) for account deposit and withdrawal (cash out) limits per transaction.

Wagering Account Withdrawals – Writer

The following delineate the withdrawal procedures for a WHUS Wagering Account with a Writer:

1. Customer provides the Writer with the account wagering account number.

2. Customer must then provide the Writer with valid identification.
3. Customer's identity is verified and customer requests withdrawal amount.
4. Writer processes the withdrawal in the Teller Terminal.
5. Teller Terminal obtains approval of the withdrawal.
6. Teller Terminal prints two tickets. One is signed by both the customer and Writer and is placed in the Writer's audit paperwork. The second is the receipt provided to the customer.
7. Writer pays customer withdrawn amount in cash.

Wagering Account Withdrawals – Kiosk

The following delineate the withdrawal procedures for a WHUS Wagering Account at a Kiosk:

1. Customer will enter their WHUS account number into the Kiosk.
2. Customer enters a personal identification number (PIN).
3. Account is verified and customer requests withdrawal amount.
4. Kiosk processes the withdrawal.
5. Kiosk obtains approval of the withdrawal.
6. Kiosk prints two tickets. One is the customer receipt and the second is the withdrawal voucher.
7. Customer presents withdrawal voucher to Writer.
8. Writer verifies Identification of the account holder.
9. Writer processes withdrawal voucher in the Teller Terminal.
10. The withdrawal voucher is signed by both the customer and Writer and is placed in the Writer audit paperwork.
11. Writer pays customer withdrawn amount in cash.

Wagering Account Withdrawals – Pre-paid card

The following delineate the withdrawal procedures for a William Hill US (WHUS) Wagering Account utilizing the William Hill Priority Access Pre-Paid Card.

1. A Customer desiring to withdraw funds from their WHUS sports wagering account for a transfer onto their William Hill Priority Access Pre-Paid Card (WHPAC) may initiate the withdrawal request using their mobile device.
2. The customer will launch the WHUS Mobile Client and log into their account using their personal identification number (PIN).
3. Once the account is verified, the customer may choose the Withdraw funds option.
4. The withdrawal window opens, and the customer enters the withdrawal amount.
5. New William Hill Priority Access Pre-Paid Card (WHPAC) holders enter the amount they wish to withdraw and click the "Confirm Amount" button.
 - a. Customer selects the William Hill Priority Access Pre-Paid Card as the payout method
 - b. Customer completes William Hill Priority Access enrollment screen.
 - c. Customer reviews/confirms withdrawal details.
 - d. Funds are transferred from the WHUS sports wagering account onto the William Hill Priority Access Pre-Paid Card (WHPAC).
 - e. Once a transfer has been completed, the customer is shown the transaction receipt and a STATUS: COMPLETE.
6. Existing William Hill Priority Access Pre-Paid Card (WHPAC) holders enter the amount they wish to

withdraw and click the "Confirm Amount" button.

- a. Customer selects the William Hill Priority Access Pre-Paid Card as the payout method.
- b. Customer confirms payment method and withdrawal amount.
- c. Funds are transferred from the WHUS sports wagering account onto the William Hill Priority Access Pre-Paid Card (WHPAC).
- d. Once a transfer has been completed, the customer is shown the transaction receipt and a STATUS: COMPLETE.

Additional Withdrawal Options

Withdrawal Process: ACH

When an ACH withdrawal request is submitted our current partner, Global Payments, will confirm a VIP Preferred account has already been opened for this patron. VIP Preferred is Global Payments method of validating KYC information and maintaining that associated information matches a particular patron. If the VIP Preferred account is not set up, the patron will need to go through VIP Preferred KYC process.

Withdrawal Process: Wire Transfer

William Hill's main priority is to insure patron satisfaction along with properly mitigating fraud and risk controls. If a patron requests withdrawal via Wire Transfer, they may be asked to provide additional documentation:

Bank Statement

- Must be legible
- Must match the name and address on the account
- Must include the last four digits of the bank account used to fund the sports book account
- Must include bank name

Driver's License

- Patrons driver's license must match name on the account

Copy of a Utility Bill

- Must be legible and valid
- Must match the name of registered patron

Promotional Contests, Tournaments, Drawings and Giveaway Programs

25. Rules for participating in WHUS promotional contests, tournaments, drawings and giveaway programs are displayed and/or available for customers to review at all participating satellite locations. Rules shall include, at a minimum: ALL conditions registered players must meet to qualify to enter or advance through the event, available prizes or awards, fee and distribution of prizes or awards based on specific outcomes.
26. Rules are followed. Changes to rules shall not be made after participants have registered.
27. Results shall be made available for the registered players to review at the same location or manner in which players registered. Results shall include, at a minimum: name of the event, date of the event, total number of entries, amount of entry fees, total prize pool, and amount paid for each winning category. The name of each winner is recorded and maintained but may not be made available to the

participants unless authorized by management personnel

28. Fees collected, less cash prizes paid, are subject to the wagering taxes pursuant to Iowa Code section 99F.11(4). In determining sports wagering net receipts, to the extent that cash prizes paid out exceed fees collected, the licensee or advance deposit sports wagering operator shall be deemed to have paid the fees for the participants
29. Compliance with all other federal, state, and local laws and rules outside of the commission's jurisdiction
30. Promotional payouts that are either deducted from gross gaming revenue, or are greater than or equal to \$500 and not deducted from gross gaming revenue, are documented to include the following:
 - a. Date and time.
 - b. Dollar amount of payout or description of personal property.
 - c. Reason for payout (e.g., promotion name).
 - d. Signature(s) of the following number of the WHUS employees verifying, authorizing, and completing the promotional payout with the customer:
 1. Two employee signatures for all payouts of \$100 or more that are deducted from gross gaming revenue;

Note: For approved computerized systems that validate and print the dollar amount of the payout on a computer-generated form, only one employee signature is required on the payout form.

2. One employee signature for payouts of less than \$100 that are deducted from gross gaming revenue; or
3. One employee signature for payouts of \$500 or more which are not deducted from gross gaming revenue.
- e. Customer's name (for drawings only).

Note: Documentation may be prepared by an individual who is not a sports book department employee as long as the required signatures are those of the employees completing the payout with the customer.

31. If the promotional cash (or cash equivalent) payouts, including those as a result of drawings and giveaway programs, is less than \$500, and are not deducted from gross gaming revenue, documentation is created to support bank accountability.

Note: Required documentation may consist of a line item on a cage or sports accountability document (e.g., "43 \$10 sports cash giveaway coupons = \$430").

32. All contest/tournament entry fees, prize payouts, participant's wagering selections and contest/tournament results are recorded in the CBS computer system.

Note: This requirement is inapplicable to contests/tournaments that do not require entry fees or other prerequisites such as a minimum amount of wagers to qualify, and therefore, these types of tournaments may be offered without recording the results in the computerized system. Note 2: Noncash prize payouts from contests/tournaments are to be completed and such payouts are not

required to be recorded in the sports computer system.

33. The contest/tournament entry fees and prize payouts are summarized and posted to the accounting records monthly.

Note: For free tournaments, the information required by the above ICS must be recorded except for the number of entries, dollar amount of entry fees and total prize pool.

34. The contest/tournament records listed above are maintained for each event.

Checkout Standards

35. The CBS system indicates the amount of net cash that should be in each Writer's station. Sports Book Writers cannot access this information. Supervisors and Managers must enter their User ID and Password to access this information.

36. For each Writer station, a summary report is completed at the end of each shift including:

- a. Amount of all transactions (tickets written, tickets voided, tickets cashed, contest payments and all other transactions) from the starting bank to the ending bank, which should match the amount of cash in the Writer's drawer at the end of the shift.
- b. On a daily basis, the Writer reconciles with the host property to reimburse the host property for the Cage paid tickets while the Sports book is closed. WHUS Audit then foots and reconciles the paid tickets from the Cage location to the CBS System Report. All variances are investigated and documented outside of Sports Book operations.

Note 1: ICS#36 is also to be performed whenever there is a change of a writer at a station during a shift. In such a case when the cash is transferred from one writer to the next writer, the cash summary report for the shift is to reflect for each writer and each station the amount of cash turn-in and any variances between the cash turn-in and the amount of net cash that the sports computer system indicates should be in each writer station.

Note 2: ICS#36 does not apply to areas outside the sports book area (e.g., casino cage) that cash tickets.

Note 3: ICS#36 does not apply to betting kiosks.

Note 4: Alternatively, ICS#35 and #36 may be performed for each writer rather than each writer station.

37. For each betting kiosk:

- a. Weekly, two employees remove the tickets and vouchers from the hopper.
- b. Weekly, two employees remove all cash from the kiosk, count and document the count.

- c. Employees, who remove the winning tickets, vouchers or cash from the kiosk, generate a report of the transactions and accountability.
- d. Weekly, when the winning tickets, vouchers or cash is removed from the kiosk, the audit department reconciles all the cash remaining in each kiosk to the cash loaded into the kiosk plus/minus cash transactions. The audit department then compares the kiosk reports to the transactions recorded by the CBS system. In addition, the cashier paid tickets and vouchers for kiosk only locations are footed daily and traced to the weekly totals. Variations are documented and investigated.
- e. Winning tickets and vouchers are delivered to the audit department.

Employee Segregation of Duties

Note: Administrative functions include setting up events, changing event data, inputting results, and assigning ID numbers to personnel.

Note: **Book Staff** writes tickets and consistently deliver an outstanding service which exceeds customer expectation and actively promotes the William Hill brand.

Note: **Operations Management** effectively manage the day-to-day activities and business levels of sports books within their assigned area, ensuring increased staff performance and efficiency through encouraging a culture of support and development.

38. Sports book employees, who write tickets, in any capacity, regardless of position or title, do not perform the function of approving voided tickets. Only Traders, who do not write tickets, perform the function of approving voided tickets in the system. In the case of a not-in-computer void, they are approved by Customer Service as stated below in 38(a) and 38(b).

- a. Supervisors do not authorize voids for any tickets. Not-in-computer voids are recorded by the Writer in the log used specifically for that purpose, indicating the Writer's name and the name of the person authorizing the void. In the event a supervisor is the only employee in the sports book, he/she will be able to write tickets, but as stated in 38, will not approve voided tickets or non-in-computer voids.
- b. The log is forwarded to the Audit department on a daily basis for a 100% audit of voids for the proper signature, a void designation on the ticket, any indications of past-post voiding, and other appropriate regulation compliance. Any discrepancies noted, and investigations performed must be documented in writing and maintained within the audit paperwork.

39. Employees who have access to an administrative terminal, or perform administrative functions, do not write or cash tickets.

Note: An employee assigned writer/cashier functions are not allowed to switch for certain shifts or

days to having administrative functions. Conversely, an employee assigned administrative functions is not allowed to switch for certain shifts or days to having writer/cashier functions

40. WHUS will immediately report to the commission any abnormal wagering activity or patterns that may indicate a concern about the integrity of an authorized sporting event or events, and any other conduct with the potential to corrupt a wagering outcome of an authorized sporting event for purposes of financial gain, including but not limited to match fixing, and suspicious or illegal wagering activities, including the use of funds derived from illegal activity, wagers to conceal or launder funds derived from illegal activity, use of agents to place wagers, or use of false identification. An investigation is then performed, completed and the outcome is forwarded to IRGC. WHUS is a member of the Sports Wagering Integrity Monitoring Association (SWIMA) to ensure that all regulatory and licensees are made aware of any suspected activity.
41. WHUS has a responsibility to protect sports integrity by identifying, preventing, combatting, and investigating the threats posed by match-fixing and betting-related corruption. Instances where sports wagering may impact sports integrity include but are not limited to: an abnormal amount of money wagered in a small or obscure market, large amounts of money wagered at a below market price, and larger amounts of money wagered on an event, relative to historic practice (collectively, “Unusual Activity”).

If a trader identifies a potential instance of Unusual Activity:

1. He or she will escalate to the Director and Assistant Director of Trading (“US Trading Management”).
2. US Trading Management will review all monies wagered on the event to analyze where the event opened, how the line transitioned, and the customer identities involved in the event wagering. US Trading Management may reach out to industry colleagues to determine whether they have had similar circumstances involving the particular event.
3. If US Trading Management deems that the Unusual Activity has an adverse impact on maintaining sports integrity, no further wagers will be accepted on the particular event.
4. US Trading Management will promptly notify the General Counsel and the Director of Compliance (“Legal & Compliance”). Details of the Unusual Activity, along with any supporting documentation will be provided.
5. Legal & Compliance will immediately notify the applicable regulators. Compliance will maintain all correspondence between William Hill US and the regulators, along with the results of the Unusual Activity investigation.
6. US Trading Management will also notify the William Hill Group Trading Director.

If a writer witnesses a potential instance of Unusual Activity:

1. He or she will escalate to his or her immediate supervisor or manager.
2. The supervisor or manager will promptly notify the Senior Vice President of Operations.
3. The Senior Vice President of Operations will escalate to the US Trading Management.
4. The same procedures will apply as noted above in steps three (3) through six (6).

Generic Passwords for Casino Cage Cashiers

42. Casino Cage personnel utilize generic passwords for the sports computer system. Cage personnel comply with the following:
- May cash winning sports wagering tickets in the Casino Cash Operations area.
 - After verifying the winning ticket in the sports computer system, the cashier or above will sign the customer's copy of the ticket, immediately date/time stamps the ticket and then maintains the cashier's drawer until such time a buy is completed, and the tickets are routed to the Employee Window.
 - The cashiers or above for the shift will use the unique date/time stamp located at the sports terminal.
 - Payouts up to \$1999.99 are to be cashed at the Casino Cage.
 - A summary sheet is prepared each gaming day which lists the total tickets cashed, the total dollar amount of tickets cashed and a Casino Cash Operations employee signature. The total of that report is then balanced to the total cashed per the sports book end-of-shift report.
 - Any discrepancies noted, and investigations performed are documented in writing and maintained.
 - A copy of the summary sheet and report will be forwarded to Casino Gaming Revenue with the shift paperwork.
 - A copy of the summary sheet, report and tickets received will be forwarded to WHUS for reimbursement to the Casino Cash Operations department.

Computerized Player Tracking Systems

Note 1: Compliance with ICS#42 - #47 is required for all computerized sports player tracking systems.

Note 2: As used in these Sports ICS, the term "point" or "points" is a generic term and refers to a representative of value awarded to a customer based upon specific criterion established by the licensee. Commonly, points are earned by customers by placing wagers or purchasing room, food, beverage or entertainment admissions. Customer accounts in a player tracking system are used to track points earned/awarded to customers.

43. The addition/deletion of points to player tracking accounts, other than through an automated process, related to actual play is documented with notes placed into the CBS system under Player Transaction Report. The Vice President of Marketing and Public Relations authorizes adjustments and Customer Support personnel perform the adjustments. The documentation of the manual change in player points is randomly verified by an employee of the Compliance department on a quarterly basis.

Note: The above ICS does not apply to the deletion of points related to inactive or closed accounts through an automated process.

44. Employees who redeem points for customers do not have system access to inactive or closed accounts without supervisory personnel authorization. Documentation of such access and approval is created and maintained.
45. Customer identification is required when redeeming points without a player-tracking card.
46. Changes to the player tracking system parameters, such as point structures and employee access, is performed by a Customer Support Lead or above, who are independent of the sports department. Documentation is generated in the CBS system and reviewed by an employee of the Compliance department on a quarterly basis.
47. All other changes to the player tracking system are documented in the Player Transactions Report and/or by CBS management.
48. Rules and policies for player tracking accounts including the awarding, redeeming, and expiration of points are available for customer review at each satellite location.

Computer Reports

Note 1: Account Wagering placed using communications technology (e.g. cell phones) is included at one book and procedures are delineated within these internal controls.

49. Adequate documentation of all pertinent sports book information is generated by the CBS system.
50. This documentation is restricted to authorized personnel. The generation of end-of-day Sports computer system reports is automated as a standard end-of-day process and is managed by the CBS Software Support graveyard team. This department is independent of the Sports department. Each report indicates the date, book's name and/or community number, and title of the report.

Note: As used in ICS#48 and #49 sports computer system report descriptions, the term "ticket description" refers to the terms of the wager as described in ICS#4.

51. Sports computer system documentation is created daily and minimally includes the following reports:
 - a. Transaction report which lists, by writer/cashier, for each write, payout and void transaction: the ticket number, transaction date and time, writer/cashier station number, writer/cashier number, transaction type, ticket description, and amount of transaction. The report lists by writer/cashier, and in total, the amount of write, voids, payouts, vouchers issued, and vouchers redeemed.

Note: The transaction report may be a combination of more than one report (e.g., one for write

and one for payouts). Wagering account transactions may be in a separate wagering account transaction report.

- b. Sports Book results report, which lists, for each event: the event date and cutoff time (as previously entered into the sports computer system), the event (e.g., team names and team identifications), and the event results/winners.
- c. Futures reconciliation report which lists the amount of, by date of event for today and future event dates: wagers written on previous days (previous write), wagers written today on future events (write today or future write), wagers written on previous days refunded today (previous canceled today), wagers written on previous days for today's event (futures back-in), and total remaining wagers written for events in the future (net write).
- d. Futures reports:
 - 1) Futures back-in ticket detail report, which lists the tickets written on previous days for events occurring today, by event, including the ticket number, ticket description and date of event. The report lists the total amount of wagers written on previous days for today's event.
 - 2) Future ticket detail report which lists the tickets written on previous days and today for events in the future, by date of event/by event, including: the ticket number, ticket description, and date of event. The future tickets detail report lists totals of the amount of wagers by date of event, by event for all tickets.
- e. Unpaid reports:
 - 1) Unpaid winners detail ticket report which lists the unexpired, winning tickets that have not been paid including: the event date, ticket number, ticket description, and amount to be paid, and payout amounts in total.
 - 2) Unredeemed voucher detail report, which lists the unexpired vouchers that have not been redeemed including: the voucher number, date of issue, and amount of voucher, and vouchers in total.

Note: Tickets and vouchers expire when the period of time the book will honor winning wagers/vouchers has lapsed usually 365 days from the DATE of event.
- f. Purge reports:
 - 1) Purge detail ticket report which lists the expired, winning tickets that have not been paid, by ticket number, including the event date, ticket number, ticket description, and amount of payout.

- 2) Purge detail voucher report, which lists the expired vouchers that have not been redeemed including: the voucher number, date of issue, and amount of voucher. The report lists total amount of vouchers to be added back into revenue.

Note: Tickets and vouchers expire when the period of time the book will honor winning wagers/vouchers has lapsed.

g. Unpaid and voucher summary reports:

- 1) Unpaid summary report which lists the amount of the beginning balance of unpaid tickets, previously unpaid tickets paid today, new unpaid tickets (i.e., unpaid ticket from event occurred today) and ending balance of unpaid tickets.
- 2) Voucher summary report, which lists the amount of the beginning balance of unredeemed vouchers, previously unredeemed vouchers, redeemed today, new unredeemed vouchers (i.e., vouchers issued today and remained unredeemed) and ending balance of unredeemed vouchers.

Note: The beginning balance is not required to be listed on the report as long as the previous day's ending balance of unpaid/unredeemed is available.

h. Wagering account reports as follows:

- 1) Daily account wagering detail report, which lists by writer/cashier station number, each transaction including writer/cashier station number, wagering account number, the transaction (e.g., wager, deposit, withdrawal), and the transaction amount. The report lists totals by transaction type.

Note 1: The daily account wagering detail report may be a part of the wagering account transaction reports or a combination of reports.

Note 2: The writer/cashier station number is not identified when the customer places a wager through a mobile device.

- 2) Daily account wagering summary report, which lists by writer/cashier station number, for wagering accounts with activity for the day, by wagering account and in total: the amount of deposits, winnings, voided wagers, wagers, withdrawals and other adjustments, tracked utilizing customer name, ID and amount. The report lists totals for write, voids/cancelled, net write payouts and net win.

Accrual basis recap report, which lists the amount of tickets written today for today's events (current write), wagers written today on future events (future write), wagers written on previous days for today's event (futures back-in), accrual write, payouts from wagers written today and paid today (current payouts), payouts paid today for events on previous days (previous payouts), unpaid winners from event occurred today (current unpaids), accrual payout, unpaid winners and unredeemed vouchers expired today (unpaids to revenue), taxable revenue, and book revenue. The accrual basis recap report is a daily and month-to-date report. Daily and month-to-date amounts may be reflected in separate reports rather than one report.

Note 1: As used in the above accrual basis recap report:

- Accrual write is equal to: current write, (+) futures back-in.
- Accrual payout is equal to: current payouts, (+) current unpaids.
- Book (accounting) revenue is equal to: accrual write, (-) accrual payouts, (+) unpaids to revenue.
- For cash basis, taxable revenue on IRGC tax returns is equal to: current write, (+) future write, (-) current payouts, (-) previous payouts, (+) expired unredeemed vouchers when vouchers were included in payout amounts.
- For modified accrual basis, taxable revenue on IRGC tax returns is equal to: accrual write, (-) current payouts, (-) previous payouts, (+) expired unredeemed vouchers when vouchers were included in payout amounts.

Note 2: Alternatively, the accrual basis recap report may include “today’s write” and “today’s payouts” rather than “current write” and “current payouts” as follows:

- Today’s write is equal to: current write, (+) future write.
- Today’s payouts are equal to: current payouts, (+) previous payouts.

i. Exception information (sorted by exception type), including:

- 1) Voids, past-post voids, in-progress voids, past-post write, in-progress write.
- 2) Changes in odds, cut-off times, results, events data.
- 3) All supervisory approvals.

52. The sports computer system documentation for wagering account activity is created on demand, and includes, at a minimum, for a day, month-to-date, year-to-date and two-year cumulative basis:

- a. Customer transaction detail report that lists, by wagering account and in total, for all wagering accounts: the wagering account number, beginning balance, each deposit, wagers and cancelled wagers (ticket number, transaction date and time, and ticket description), winning wagers (ticket number, transaction date and time, ticket description, and payout amount), net win, withdrawals (date and amount), adjustments (date and amount), and ending balance.
- b. Customer transaction summary report that lists, by wagering account and in total, for all wagering accounts: the wagering account number, customer’s name, beginning balance, deposits, amount of wagers (write and cancelled wagers), amount of winning wagers, net win, withdrawals, adjustments, and ending balance.

Note 1: All wagering accounts regardless of account balance must be included on the customer transaction summary report.

Note 2: Daily, month-to-date, year-to-date, and two-year cumulative amounts may be reflected in separate reports rather than one report.

Accounting/Audit Standards

53. The sports book audit is conducted by Audit personnel, which is independent of the sports book operations.

Note: Such personnel may also perform the audit function for the outstation book of affiliated properties (and vice versa).

54. Once per quarter, for each betting kiosk, Audit personnel foots the winning tickets and vouchers redeemed for a week and trace the totals to the totals recorded in the sports CBS system and the related accountability document. This procedure may be performed for different kiosks throughout the quarter as long as each kiosk's activity is examined once per quarter. The tests and the results of investigations into all variances by kiosk are documented and maintained.

Note: This procedure may be performed by non-accounting personnel as long as the individual has not performed the reconciliation required by ICS#53.

55. For manned locations, annually, for one day, Audit personnel will foot the write on the restricted computer system record of written tickets for a minimum of three writers for each sportsbook and three writers for each sports pool for one day and trace the total to the total produced by the CBS system.

56. For manned locations, Audit personnel foot the customer copy of paid tickets for a minimum of one writer station per month and traces the totals to those produced by the CBS system.

57. For manned locations, annually, for one day, Audit personnel foot the redeemed vouchers for one writer station and trace the totals to those produced by the CBS computer system.

58. Daily, the write and payouts at the books (except for betting kiosks) are compared to the cash reconciliation. Large variances are investigated and documented.

59. Daily, reconcile the dollar amount of WAT in and WAT out per the WAT by Gaming Area report to the transaction report. Any variances noted are investigated and documented.

60. Daily, select a random sample of 5 paid transactions from the sports computer system transaction report and trace the transaction to the customer's copy of the paid ticket for all manned locations. This procedure is done weekly for every Kiosk only location.

- a. The tickets are recalculated and re-graded using the computer record of event results.
- b. The date and starting time of the event per the results report are compared to the date and time stamp on the ticket and in the computer sales/transaction report.
- c. The terms of the wagers (e.g., point spreads, money-lines, etc.) per the computer sales/transaction report or per the results report (if that summary lists all point spreads and money lines at which wagers were written or if an equivalent report satisfying this requirement is produced) are reviewed

and compared to an independent source for extravagant or questionable activity.

Note 1: For sports book winning tickets and parlay card tickets, the terms of the wagers can be compared to an independent source such as a newspaper (or its website), sports league website, a licensed sports information service or other reputable source.

61. Daily, accounting/audit personnel, for payouts made without sports computer system authorization at the time of payment including such payouts for contest/tournament winners, will: Trace all payouts to the sports computer system transaction report or the purged tickets report to verify authenticity of the initial wager, For payouts subsequently entered into the sports computer system by sports personnel, compare the manual payout amount to the sports computer system amount and For payouts not entered into the sports computer system by sports personnel, enter the payout into the sports computer system and compare the manual payout amount to the sports computer system amount. If the system is inoperative, manually regrade the ticket to ensure the proper payout amount was made.

Note: Appeasement payments (e.g., non-winning ticket payouts resulting from a customer complaint or employee error) are not deductible from gross revenue.

62. Daily, the sports computer system's summary of events/results report is traced to an independent source for 5% of all sporting events to verify the accuracy of starting times (if available from an independent source) and final result.

Note: The starting times for sporting events and races that are wagered on in conjunction with a tournament or contest is included in population from which the 5% sample is chosen.

63. Daily, for all voided tickets:

- a. The computer reports, which display voided ticket information, are examined by Audit/Accounting to verify that tickets were properly voided prior to the cutoff times for event wagering.
- b. The voided tickets are examined for a void designation and proper signatures, and for not-in-computer voids, the date and time stamp on the ticket for the time of the void.
- c. For a sports computer system that prints void tickets, the void ticket is attached to the original ticket.

64. System exception reports are reviewed on a daily basis by Audit personnel for propriety of transactions and unusual occurrences in changes to the personnel access listing, changes in odds, cut-off times, results, tickets written for events in-progress, void authorizations and changes to event data. Any investigation performed regarding the exception reports is documented.

Note: An exception report is defined as a report produced by the computerized system identifying unusual occurrences, changes to system configuration parameters, alteration to initially recorded data, voids, etc.

65. One day per month, the sports computer-generated reports are reviewed to ensure it maintains the necessary outstanding sports wagering liability. An accounting of this reserve is calculated as follows

and will be made available for inspection to the commission upon request.

- a. Amounts held by the book for customer wagering accounts;
- b. Amounts accepted by the book as wagers on events whose outcomes have not been determined (futures); and
- c. Amounts owed but unpaid by the book on winning wagers through the period established by the book for honoring winning wagers (unpaid winners and unredeemed vouchers).

Note: WHUS cash reserve is maintained in a separate bank account segregated by state and utilized for reserve purposes only including “same bank transfers” to increase or decrease to match the liability.

66. At least once per quarter, Audit/Accounting personnel:

- a. Recalculate and verify the change in the unpaid winners and unredeemed vouchers balance to the total purged tickets and vouchers.
- b. If future wagers are accepted, review the sports computer system reports to ascertain that future wagers are properly included in write on the day of the event.

67. Compliance reviews all wagering multiple transaction logs that have been prepared by the sports book’s reports have been completed for all reportable transactions.

68. Monthly, Accounting reviews all contests, tournaments, promotional payouts, drawings and giveaway programs to determine proper accounting treatment and proper win/loss computation.

69. The following documentation is maintained for all contests, tournaments, promotional payouts, drawings, and giveaway programs (including payouts from computerized player tracking activity):

- a. Copies of the information provided to the customers describing the contests, tournaments, promotional payouts, drawings, and giveaway programs (i.e., brochures, flyers).
- b. Effective dates.
- c. Accounting treatment, including general ledger accounts, if applicable.
- d. For tournaments and contests, the dollar amount of the prize pool. Additionally, if applicable, include the amount of contributions to the prize pool by customers and the amount supplemented by the licensee.
- e. For tournaments and contests, the name of the organizations (or persons) that conducted the contest/tournament on behalf of, or in conjunction with, the licensee, if any. The extent of responsibilities (including ICS compliance responsibilities) each organization and the licensee had in the contest/tournament (e.g., ABC nonprofit is to receive 100% of the entry fees and provide noncash prizes for the winners with the licensee collecting entry fees, operating the tournament and distributing prizes to winners) will also be documented.

70. Daily, Accounting reconciles all contest/tournament entry and payout forms to the dollar amounts recorded in the appropriate accountability document and computerized system report.

71. Payments made to the winners of a contest/tournament are reconciled by Compliance with the contest/tournament entry fees collected to the actual contest/tournament payouts made. This reconciliation determines whether the entry fees collected, the payouts made, and the amounts withheld, if applicable, were distributed in accordance with the contest/tournament rules.
72. Monthly, reconcile the total amount of WAT in and WAT out per the WAT Summary report to the month-end accrual basis recap report. This reconciliation is documented and maintained. All variances are reviewed, documented and maintained.
73. All taxes and fees, whose collection by the state is authorized under Iowa Code chapters 99D and 99F, shall be accounted for on a fiscal-year basis, each fiscal year beginning on July 1 and ending on June 30.
74. Submission of sports wagering net receipts taxes, A tax is imposed on the sports wagering net receipts received each fiscal year from sports wagering. Sports wagering net receipts means the gross receipts less winnings paid to wagerers on sports wagering. Any offering used to directly purchase a wager shall be considered receipts for the purpose of this calculation. Voided and cancelled transactions are not considered receipts for the purpose of this calculation.
75. All moneys collected for and owed to the state of Iowa under Iowa Code chapter 99F for the payment of sports wagering taxes shall be accounted for, itemized and paid on a monthly basis by the 15th of each month in a format approved by the commission.
76. For sports computerized player tracking systems, Compliance will perform the following procedures at least one day per quarter:
 - a. Review all point addition/deletion authorization documentation, other than for point additions/deletions made through an automated process, for propriety.
 - b. Review exception reports including transfers between accounts.
 - c. Review documentation related to access to inactive and closed accounts.
77. Annually, the computerized sports player tracking system (CBS) is reviewed by the Audit Manager, who is independent of the individuals that set up or make changes to the system parameters. The review is performed to determine that the configuration parameters are accurate and have not been altered without appropriate management authorization. The system will also be tested, if possible, to further verify the accuracy of the configuration parameters (e.g. simulate activity to verify the accuracy of the amount of points awarded). The test results are documented and maintained.
78. All documentation (e.g., log, checklist, notation on reports, and tapes attached to original documents) is maintained evidencing the performance of the Audit procedures, the exceptions noted, and follow-up of all Audit exceptions is maintained.
79. Unclaimed winnings and abandoned accounts are subject to the following requirements:

- a. Unclaimed winnings of over 90 days at the close of a licensee's fiscal year shall be disallowed as a deduction from gross receipts for the calculation of sports wagering net receipts for the sports wagering tax.
- b. Player accounts abandoned or inactive under this rule, unless otherwise subject to Iowa Code chapter 556, for longer than 36 months will be remitted to the state of Iowa unclaimed property division in accordance with Iowa Code chapter 556.
- c. Player accounts are considered abandoned or dormant if no activity by the account holder has occurred for 36 consecutive months. Player activity includes making a wager, making an account deposit or withdrawing funds.
- d. Written notice must be provided to a player after 30 months of no activity has occurred. The notice shall include, but not be limited to, a statement that abandoned or inactive accounts will be submitted to the state of Iowa as unclaimed property after 36 months.
- e. No licensee or advance deposit sports wagering operator shall charge an administration fee or maintenance fee for any dormant player account derived from state of Iowa residents at any time for any reason.

Payout Procedures for Mail-In Winning Sports Tickets and Vouchers

80. Audit/Accounting, or Receptionist, located at corporate offices, and independent of the Sports Book operations, receive the original winning race/sports tickets and vouchers.
81. The above-mentioned personnel record the winning sports tickets and vouchers on a log as a mail pay. The log includes the date received, customer's name, sports ticket or voucher number, the date the ticket/voucher is processed in the system, and the date the check is mailed. The ticket is then stamped "MAILPAY."
82. The winning tickets and vouchers are entered into the system by Audit/Accounting and/or Customer Support personnel for validation and cancellation.
83. An Audit employee compares the "paid" winning sports tickets and vouchers to the mail pay log and the system report for paid winning sports tickets and vouchers. Any discrepancies are documented and reviewed with sports accounting management.
84. An Accounting/Audit employee, independent of the individuals who processed the mail pay winning tickets and vouchers, reviews the customer's correspondence submitted, the winning tickets and vouchers, the mail pay log and the computer system report for "paid" winning sports tickets and "paid" vouchers for any discrepancies. All discrepancies are documented and resolved prior to remitting the proper amount to the customer.

Prohibited Patrons

The following patrons are prohibited from wagering in the state of Iowa: coaches, athletic trainers, officials, players, or other individuals who participate in an authorized sporting event, by persons who are employed in a position with direct involvement with coaches, players, athletic trainers, officials, athletes or participants in an authorized sporting event in which wagers may be accepted. Patrons are required to acknowledge upon account creation that they do not fall into a prohibited category. As noted in house rules.

Self-Exclusion

William Hill employees will be mandated to take the Company's Responsible Gaming Training. This training will be refreshed on an annual basis.

By the end of William Hill's Responsible Gaming training, Iowa employees will be able to:

- a. Understand the importance of Responsible Gaming to William Hill It's mission and commitment to integrity.
- b. Know the importance of an employee's role with regard to responsible gaming.
- c. Understand the definition, and signs and symptoms of problem gambling and those it affects.
- d. Understand the impact on our customers and business if we don't encourage responsible gaming.
- e. Understand measures William Hill has in place to prevent problem gambling and protect the player.
- f. Identify the triggers to spot a player with a potential problem and effective way to positively intervene.

William Hill employees will also be educated on problem gambling warning signs as outlined under the Gambling tab on yourlifeiowa.org/gambling.

William Hill employees shall take reasonable steps to inform WHUS customer service of suspected at-risk behavior in an effort to review the patron's previous wagering activity and monitor future transactions.

Responsible Gaming materials will be made available and on display for the patron at the Sportsbook (i.e. brochures and signage).

WHUS also participates in a voluntary self-limiting program, which allows our customers to limit themselves from wagering activities. If a customer requests to limit themselves from placing wagers at a Book, they may complete the William Hill US Self-Limit Request form and return to any employee. Once an employee receives the Self-Limit Request form, they should scan to Compliance and forward the original in the Accounting Audit envelope to be processed.

WHUS will download new and reinstated exclusion information from the IRGC self-exclusion system on a scheduled weekly interval to ensure the patron data base is reviewed and updated accordingly within the (7) calendar day requirement.

Once the patron has been successfully added to the voluntary Self-Exclusion list the following procedure should be followed:

1. The patron's wagering and/or rewards club account(s) will be reviewed to ensure the patron does not have any active wagers.
2. In the event the patron has active wagers, the Trading team and Customer Support team will be contacted to lock and void such wagers.
3. The patron will be contacted via phone, email, and/or certified mail, stating the open wagers have been voided and will be refunded via a certified check sent to their address on file within fourteen (14) business days.

4. The patrons name will be removed from any marketing promotions/mailings within 90 days after enrollment in the self-exclusion program.
5. In the event of an indefinite self-exclusion or if the individual enrolls in the statewide program, WHUS must ensure that the patron is paid in full for their account and all user profiles will be deactivated.
6. Writers are to refuse to accept a wager or allow the purchase of any gambling product approved by the Office to any individual that has been identified or suspects as being on the voluntary Self-Exclusion list.
7. The retail team is to promptly notify the Office, WH Compliance, WH Responsible Gaming and WH Management before close of business hours that day that an individual on the voluntary Self-Exclusion list had attempted to place or is discovered to have placed a sports wager.
8. Deny a person on the voluntary Self-Exclusion list from any winnings derived from sports betting. The retail team should, where reasonably possible, confiscate from the individual in a lawful manner, or notify a security officer to confiscate, or refuse to pay any such winnings derived from sports betting.

William Hill acknowledges that it will be provided electronic access to names and social security numbers of persons voluntarily excluded through a secured interactive internet site maintained by the Commission and information regarding persons voluntarily excluded shall be disseminated to William Hill.

William Hill acknowledges that the names, social security numbers, and information regarding persons voluntarily excluded shall be kept confidential unless otherwise ordered by a court or by another person duly authorized to release such information.

William Hill acknowledges that the person requesting to be voluntarily excluded will be provided information compiled by the Iowa department of public health on gambling treatment options.

The state and William Hill under this chapter or chapter 99D shall not be liable to any person for any claim which may arise from this process. In addition to any other penalty provided by law, any money or thing of value that has been obtained by, or is owed to, a voluntarily excluded person as a result of wagers made by the person after the person has been voluntarily excluded shall be forfeited by the person and shall be credited to the general fund of the state.

Patrons may close/deactivate their remote/retail wagering account, and terminate any associated email, by submitting a request to us at contact@williamhill.us in the manner set forth in our Terms and Rules.

WHUS will check a patron name and social security number against the IRGC database system:

- a. When an individual patron cashes in or cashes out \$10,000 or greater in aggregate in a gaming day,
- b. When an individual patron cashes check(s) of \$10,000 or greater in aggregate in a gaming day,
- c. When an individual patron wins a taxable jackpot,
- d. Prior to paying a marketing/promotional winner when it is a tax reportable amount, and
- e. Prior to paying a tournament winner when it is a tax reportable amount.

WHUS website and mobile application will include the IRGC website <https://irgc.iowa.gov/self-exclusion-program>.

Offset Program Requirement

For all taxable gambling winnings reported on form W2G payout, an electronic offset search will be conducted via winner's SSN to determine if there are any valid liens. If a match is found the hold amount will be entered for the amount of the winnings up to the maximum amount owed. All taxes are to be taken from winnings before money is held for the offset program. Two letters will be generated, one for the winner and the other for internal purposes. Payments for any offsets will be remitted to the state on a weekly basis.

Global Risk Management

WHUS complies with all federal laws and regulations. For compliance with the Bank Secrecy Act and its implementing regulations, please see WHUS' AML Program.

Annual Audit Requirement

An audit of the advance deposit sports wagering operations for the advance deposit sports wagering operator or licensee or parent company of the advance deposit sports wagering operator or licensee, shall be conducted by certified public accountants authorized to practice in the state of Iowa and provided to the commission within ninety days of the licensee's fiscal year, meeting the following conditions:

- a. Inclusion of an internal control letter, audited balance sheet, and audited profit-and-loss statement including a breakdown of expenditures and subsidiaries of advance deposit sports wagering activities.
- b. Inclusion of a supplement schedule indicating financial activities on a calendar-year basis if the advance deposit sports wagering operator or licensee's fiscal year does not correspond to the calendar year.
- c. Report of any material errors or irregularities that may be discovered during the audit.
- d. Availability, upon request, of an engagement letter for the audit between the advance deposit sports wagering operator or licensee or parent company of the advance deposit sports wagering operator or licensee and the auditing firm.

Information Technology Controls

Definitions

“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.

“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 gaming and entertainment systems. The term does not include user terminals.

“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 gaming and entertainment systems and applications. User accounts established by/for and used by manufacturers of the system for vendor support purposes are not considered 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” is an entity unaffiliated with a licensee, registered with the commission, and hosting on its premises any part(s) of regulated hardware or software.

“IT personnel” are employees of the licensee/operator or an IT service provider who are independent of the gaming and entertainment department; 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.

“IT service provider”, for gaming systems, is a person or an entity engaged by the licensee, and licensed, to provide management, including system administration, user access administration, support, security, or disaster recovery services for commission regulated hardware or software. For live entertainment, an IT service provider may be engaged by a licensee/operator to administer an entertainment tax related application/system (box office system or POS system) for handling and recording live entertainment taxable admission, F&B, merchandise and any other sales.

“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):

- 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);
- Modify operating system, database, and application security and policy parameters;
- Add, change, or delete system exception logging information; or
- 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 deletes 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 separation of duties.

“Vendor supported system” is one type of critical IT systems and equipment where the source code is supported solely by the manufacturer of such system. The manufacturer support of source code does not include performing the function of a “system administrator” or a “user access administrator” when the system is in use by the licensee.

Physical Access and Maintenance Controls

Note: WHUS has one computer system for sports book operations: Computerized Bookmaking Systems, Inc. (CBS), which is wholly owned by American Wagering Inc.

1. Critical IT systems and equipment for the CBS system are housed in an offsite Data Center (DC) in Iowa with access restricted to authorized employees. All systems are secured to restrict access to sports employees. The Virtual Sports PC is secured inside the PC lockbox and is located within the sports book area that is only accessible by authorized casino and WH employees.
 - a. The CBS System infrastructure is connected to a redundant power source which includes a data-center provided Uninterruptible Power Supply (UPS) backed by a diesel-generator should a loss of primary power source occur.
 - b. The Data Center, which houses all CBS System servers and related infrastructure, is supported by 24/7 security on site with access control managed via electronic key cards and biometrics. The Virtual Racing (VR) PC lockbox is only accessible by using traditional key locks. Keys are secured by casino security for each Virtual Racing location. WH employees follow the casino location’s security procedures and logging to obtain the keys for the VR lockbox.
 - c. The administration of the electronic security systems, which includes 24/7 security monitoring,

bio- metric reader, security card reader and physical man trap, used to secure the CBS System at the primary Data Center, are managed by a third-party vendor, independent of the gaming department.

Note: The written system of internal controls is to delineate the methods, processes and practices.

2. Access to rooms housing critical computer systems as stated in #1 is restricted to authorized personnel. Lists of authorized personnel are managed by the Director of IT & Cybersecurity. Requests for access are submitted and reviewed by Director of IT & Cybersecurity and if access is granted, a request is made to the third-party data center facility to add the user to the approved access list.
3. Access to the production Data Center by non-IT personnel is documented and maintained by data center staff and includes:
 - a. The name of the visitor(s)
 - b. Time and date of arrival
 - c. Time and date of departure
 - d. Reason for visit
 - e. The name of the IT personnel authorizing such access

System Parameters

4. The computer systems, including gaming related application software, are logically secured with passwords. Security passwords are configurable and 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 must contain a combination of the following criteria: uppercase letters (A to F) and/or numeric (0-9).
 - c. Passwords may not be re-used for a period of 18 months; or passwords may not be re-used within the last ten password changes.
 - d. User accounts are automatically locked out after 3 failed login attempts. Once an account is locked, a user can contact the Customer Support Department to speak with an agent. After verifying user's identity, a Customer Support Agent will assist in unlocking the user's account.

Note 1: The written system of internal control is to delineate whether the system is configurable for security parameters for passwords, and to what extent the system is configurable in meeting the security parameter requirements.

Note 2: ICS #4 does not apply to service accounts and generic user accounts.

Note 3: For ICS #4(d), the system may release a locked-out account after 30 minutes has elapsed.

5. System event logs and/or reports for applications and servers are configured to track the following events:

CBS Sports System Application

- a. Failed login attempts.
- b. Not configurable in the CBS System.
- c. The CBS Sports System records changes made to relevant system parameters and they are accessible in the Daily Exception Report.
- d. Audit trail of information changed by administrator accounts is generated by the system and includes the following:
 - 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. Not configurable in the CBS

System. OpenVMS Operating System

User accounts and passwords utilized on OpenVMS are all generic system and/or service support accounts. Users do not currently login to OpenVMS systems by user-specific usernames.

- a. Failed login attempts are logged in the Accounting Log File.
- b. Not configurable – The native data storage technology utilized by the CBS application is called RMS and does not provide OS-level auditing capabilities.
- c. Changes to OpenVMS operating system parameters are logged in the Operator Log File.
- d. Not configurable in the OpenVMS operating system.
- e. Date and time changes from the master time server are logged in the Operator Log File.

Linux Operating System

- a. Failed login attempts are logged by the operating system.
- b. Where relevant, changes to live data files occurring outside of normal program and operating system execution are logged by the operating system. However, the CBS Sports System does not currently store gaming data directly on a Linux-based operating system.
- c. Changes to Linux operating system parameters are logged in the Operator Log File.
- d. Not configurable in the Linux operating system.
- e. Date and time changes from the master time server are logged by the Linux operating system.

MySQL Database System

- a. Failed login attempts are logged by the MySQL.
- b. Changes to live data files occurring outside of normal program and operating system execution are logged by MySQL.
- c. Changes to MySQL system parameters are logged in the MySQL Log File.
- d. Audit trail of information changed by administrator accounts is generated by MySQL and includes the following:
 - i. Account login name;
 - ii. Date and time of event;
 - iii. Description of event;
 - iv. Not configurable in MySQL
 - v. Not configurable in MySQL
- e. Date and time changes from the master time server are logged by the Linux operating system.

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).

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 gaming and/or entertainment systems.

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

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

Note: For ICS #5, 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 the system is configurable, in tracking specified events.

6. The activity logs for the events listed in above ICS #5(a) through (c) and (e) are maintained by WHUS for a minimum of seven days and the activity logs in ICS #5(d) are maintained for a minimum of thirty days.
7. Daily CBS System event logs are reviewed at least once a week (for each day of the entire previous week) by Accounting/Audit personnel, for events listed in ICS #5. Evidence of this review is in the form of a checklist and is maintained for a minimum of 90 days. This checklist includes the date, time and name of individual performing the review, the exceptions noted, and any follow-up of the noted exception.

Note 1: For this Standard, an automated tool that polls the event logs for all gaming and entertainment related servers and provides the reviewer with notification of the above may be used. Maintaining the notification for 90 days 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. Not applicable – the CBS System does not have an automated tool, which applies to this Note.

Note 2: IT personnel who review the logs are independent of the system administration and user access administration functions and do not have system access to perform any administrative functions in the systems for which the logs are being reviewed. Alternatively, the licensee/operator 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. WHUS has designated a member of the Audit team to perform the review of ICS #7.

Note 3: This Note does not apply to WHUS. If an IT service provider maintains and administers gaming and entertainment related systems on behalf of the licensee/operator:

- The review of the logs is to be performed by IT personnel who are employees of the licensee/operator; or
- If an automated tool is used as discussed in Note 1, the notification is to be provided to IT personnel employed by the licensee/operator.

8. Exception reports produced by the CBS system are reviewed by the Accounting/Audit department. The system exception report includes, but is not limited to, changes to system parameters, corrections, overrides, over-the-limit cashes, over-the-limit write, voids, line changes, password changes, user account changes including inactive account status. The reports 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.

Note: This written system of internal control is to indicate the system's capability or lack thereof in producing an exception report documentation and to what extent this report provides specified information.

User Accounts

Note: ICS #9 through #15 in this section apply to an application level, unless otherwise specified.

9. A designated Manager within the Customer Support Team and their designated Agents review and assign CBS user accounts for new employees. Customer Support Management provisions CBS user accounts, which consists of assigning application functions matching the employee's current job responsibilities, unless otherwise authorized by management personnel, to ensure adequate separation of duties.
10. The designated Manager within the Customer Support Team and their designated Agents provision CBS user accounts for employees who transfer to a new department or location. Any previously assigned application function access for the employee's CBS user account, not applicable to the user's new role, is disabled prior to the employee accessing their new user account profile for their new role or position in a new department.
11. User access listings produced by the system include, at a minimum:
 - a. Employee name and classification.
 - b. CBS User login name.
 - c. Full list and description of application authorizations that each user account may execute.

Note: This list for ICS #11(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. Classification of user account.

Note 1: The written system of internal control is to indicate the system's capability of producing a user access listing and to what extent the system's listing provides specified information.

Note 2: The user access listing is not required for entertainment tax related applications.

12. If multiple user accounts for one employee per application are used, only one of those user accounts may be active (enabled) at a time if the concurrent use of the multiple accounts by that employee could create a deficiency in segregation of duties, which would result in noncompliance. In addition, the user account will have a unique prefix/suffix to easily identify which users have multiple user accounts within the CBS application.
13. Customer Support Management or designee is notified by Human Resources within two business days when an employee is no longer employed. Upon notification, Customer Support Management or designee changes the status of the employee's CBS user account from active to inactive (disabled) status.

Note: The reasonable period in notifying the system administrator to change the status of the terminated employee's user account assumes that it is relatively unlikely the employee will have unauthorized access to a user terminal during that time.

14. WHUS' policy does not allow remote access to the CBS System unless there are emergency circumstances, however, in the event that an employee with remote access capability is terminated, Human Resources will notify Corporate IT within one business day and Corporate IT staff will disable employee's remote access (i.e. VPN) capability.

Note: During the period of time when the employee is no longer employed and until the user, account has been disabled, it is assumed that it is relatively unlikely the employee will have unauthorized remote access to the system during that time.

15. Once per quarter, a Compliance employee reviews the user access listing for the CBS System. 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 a log of the identified user 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, the following is reviewed to 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 designated two business day 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 ICS #4(a)].

- e. There are no inappropriate assigned functions for "classification" groups assigned to a user.

Note 1: ICS #15(e) applies to a review of the assigned functions for the selected user account with group membership.

Note 2: The required review of user access listings does not apply to user access listings for any entertainment tax related applications.

Note 3: 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
- Generates any other records required by the licensee's system of internal control.

WHUS User Access Control Metrix is noted in Appendix A.

Generic User Accounts

16. Generic user accounts at the operating system level are utilized and are managed by CBS Software Support and IT Department staff. Access to each account is restricted by employee job function. For example, the generic user account "MENU" is utilized by staff requiring application level access to the CBS System and following login, the CBS application login screen is automatically displayed. Other generic user accounts, BASEEXAM, HIGHEXAM, PROGRAM and SETUP are utilized by IT and CBS Software Support staff and they provide access to operating system tools used to monitor and manage the CBS application and related core processes. Passwords for BASEEXAM, HIGHEXAM,

PROGRAM and SETUP are changed at least once every 90 days. In addition, the generic user account “MENU” is 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 controls delineates the method used to secure generic accounts.

17. Use of generic user accounts to login directly to the CBS application is not allowed, with the exception of CBS Software Support staff as part of troubleshooting a system issue. When an issue requires investigation at the application-level, CBS Software Support staff initiates a special command called “RUN SUPPORT”. This utility allows a temporary generic user account to be created and allows the support staff access to the CBS Application. Accounts created by RUN SUPPORT are identified in the daily EXCEPTION report for audit purposes.

Service & Default Accounts

18. Service Accounts 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. Service account login and password information is restricted to CBS Software Support and IT Department staff. Service Accounts are managed by CBS Software Support and IT Department staff. Where able, passwords are changed at least once every 90 days and upon termination of CBS Software Support or IT Department staff.

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.

19. 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. Default accounts are managed by CBS Software Support and IT Department staff.
20. Any other default accounts that are not administrator, service or guest accounts are disabled unless they are necessary for proper operation of the system. Where able, passwords for these accounts are changed at least once every 90 days.

Administrative Access

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

- Add, change, or delete user accounts and associated user provisioning
- Modify operating system, database, and application security and policy parameters
- Add, change, or delete system exception logging information
- Add, change, or delete permissions to data files and folders

21. Access to administer the network, operating systems, database security and system parameters is the responsibility of the Corporate IT Department with delegated limited rights given to CBS Software Support and CBS Operations staff.
22. A daily confirmation is conducted of the Virtual Sports Controller Server security access logs, by the Legal Compliance Officer, to ensure that only the authorized user account and split-password method is being used when accessing the Virtual Sports Server. The security access logs are maintained in a Remote Logging System (i.e., “Splunk”).

Note: ICS #22 requires a review to confirm that the system administrator level access is not achieved without the presence and participation of at least two individuals. The requirements include split passwords, dual keys or any other suitable method approved by the chairperson.

Backups

23. Daily backup and recovery procedures are in place and include:
 - a. Application data.
 - b. Application executable files.
 - c. Database contents and transaction logs.
24. Upon completion of the backup process, the backup media is transferred to a location separate from the location housing the servers and data being backed up. Once a week, the backup tape media is sent offsite to a third-party hosted storage location. The storage location is secured by 24/7 surveillance and physical security devices such as mantraps to prevent unauthorized access. Only authorized users, who have valid security badges, are able to access stored media. Authorized access is reviewed and granted by the Director of IT & Cybersecurity. The third-party facility provides adequate protection, via fireproof vault, to prevent the permanent loss of any data.
25. Backup system logs are reviewed daily by an IT System Engineer and CBS Software Support staff to ensure that backup jobs execute correctly and on schedule. The backup system logs are maintained at minimum for the most recent 30 days.

26. CBS and IT Department management are responsible for maintaining documentation indicating the procedures implemented for the backup processes and for restoring data and application files.

Note: While not mandatory, licensees are encouraged to test recovery procedures at least annually.

Recordkeeping

27. A listing of all regulated systems (hardware and software) including the system name and version identifier (including period of time each version was in use), related operating system and database software and hardware (including version identification and period of time each version is in use) is maintained by the Chief Technology Officer (“CTO”). System documentation for all listed in-use versions of applications, databases, network hardware and operating systems is maintained, including descriptions of hardware and software, operator manuals, etc.
28. CBS System Administrators maintain a current list of all enabled generic, system and default accounts. The documentation includes, at a minimum, the following:
- a. Name of system (i.e., 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: If the operating system and/or database support more than a single gaming or entertainment application, then the list should include all system, generic or default accounts enabled on that operating system or database, regardless of the system they pertain to.

29. IT service providers, which may from time to time be used for support, do not have direct access to CBS or related systems. If remote access is required, an IT System Engineer utilizes remote screen sharing tools such as Citrix GoToAssist and the remote session is logged and recorded.
30. The current lists required by ICS #28 are reviewed by CBS Software Support Management, in addition to the system administrator, at least once every six months. The list required by ICS #28 is reviewed to identify any unauthorized or outdated accounts.
31. User access listings (requirements listed at ICS #11) for the CBS System are retained and provide data for at least one day of each month for the most recent five years. The list of users and user access for the CBS System is in electronic format and can be analyzed by analytical tools.
32. The Director of IT & Cybersecurity maintains current documentation with respect to the network topology, deployment of servers housing applications and databases, and inventory of software and

hardware deployed and is available upon request.

Electronic Storage of Documentation

33. CBS System Reports are stored on secure network file servers maintained by IT Department staff. Users requiring access are granted “read only” access to the network file share location.

Documents may be scanned or directly stored to unalterable media (secured to preclude alteration) 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 casino department and date. This index must be available upon request by the commission.
- c. Upon request by Board agents, 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. At least quarterly, accounting/audit personnel review a sample of the documents on the storage media to ensure the clarity and completeness of the stored documents.

Network Security and Data Protection

34. Guest Wi-Fi Internet services are available and such network is logically segregated from the production network used by the CBS System.
35. The production networks serving the CBS Sports Systems are secured from outside traffic by a series of firewalls, routers and switches. In addition, the network is segmented into logical VLAN's, which are isolated from one another via firewall rules. Devices requiring access from one VLAN to another require an exception rule to be applied to the firewall, which only allows specific IP Addresses, Ports and Protocols to pass through. The Director of IT & Cybersecurity manages this process overseeing the IT Department.

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.

36. Network shared drives containing application files and data for all regulated software are secured such that only authorized personnel may gain access.
37. The Virtual Sport ViewerPC's, located at sports book sites, are secured within a locked security cage and console is not directly accessible to unauthorized personnel.

38. Corporate network devices are protected by login accounts and passwords and access is restricted to authorized IT/CBS personnel only. The login accounts meet the security parameters of IT ICS #4 and are immediately disabled when IT/CBS personnel are terminated.
39. The Director of IT & Cybersecurity maintains documentation delineating the policies and procedures established to protect a customer's personally identifiable information, including, but not limited to:

Note 1: "Personally identifiable information" means any information about an individual maintained by a licensee 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 is to be delineated in the written system of internal controls. The documentation is to be made available upon request by authorized internal and external auditors and by IRGC 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 customer 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 commission; and
- h. Provision for compliance with all local, state and federal laws concerning privacy and security of personally identifiable information.

Remote Access

40. Vendors, which may from time to time be used for remote support, do not have direct remote access to CBS or related systems. If remote access is required, IT Department and/or CBS Software Support staff utilize remote screen sharing tools such as Citrix GoToAssist and the remote session is logged and recorded.
 - a. Remote sharing sessions, utilizing tools such as Citrix GoToAssist, are logged and recorded.
 - b. Remote access to the Virtual Sport Controller Server utilizes a remote screen sharing tool such as Citrix GoToAssist and all remote sharing sessions are logged and recorded.
 - c. Remote sharing sessions, utilizing tools such as Citrix GoToAssist, are authorized by IT and CBS Software Support personnel.
 - d. Direct remote access to CBS and related systems by vendors is not allowed.
 - e. The personnel involved and procedures performed to ensure the method of establishing remote access connection to the system when the vendor requires access to the system through remote access.
41. 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.
42. Remote access for all vendors is enabled only when approved by authorized IT personnel.
43. If remote access to the production network (live network) is available and allows access to gaming and entertainment tax related 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 performing access. Remote access to the Virtual Sport Controller Server utilizes a remote screen sharing tool such as Citrix GoToAssist and all remote sharing sessions are logged and recorded

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

44. Documentation is maintained delineating a comprehensive and robust change control process to prevent any unauthorized changes being incorporated into the production environment. Changes to the production environment are controlled by the CTO. This process includes at a minimum:
 - a. All changes to controlled regulatory processes within the platform require Independent Testing Lab approval. ITL engineers will review the proposed changes and will test appropriately to ensure the change meets or exceeds regulatory requirements. Once approved, the ITL will issue a certification letter.

- b. Proposed changes to the production environment are reviewed and approved by the CTO prior to implementation;
- c. Proposed software changes are properly and sufficiently tested prior to implementation into the production environment. Actions include, describing procedures required to bring the program into service (e.g. conversion of data, installation procedures, etc.), performing and documenting quality assurance testing, and documenting user procedures as applicable.
 - 1. Testing performed would include functionality, integration, smoke, regression, and user acceptance (if required), and bug fixes or enhancements (modifications) are stored in our tracking and documentation software (Jira/Confluence). In addition, all test cases performed along with testing steps, expected and actual results, are recorded as any issues are migrated through our development and testing environments. User ID's, comments, test history, and any associated tickets are automatically tracked within our software as mentioned above.
- d. 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;
- e. 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 gaming and entertainment applications.

Information Technology Department

- 45. IT department is independent of all gaming and all operational departments. The IT department (CTO) reports directly to the CEO.
- 46. IT personnel are precluded access to wagering instruments and gaming related forms.

In-House Software Development

- 47. Source code is developed and modified in-house for the CBS Sports System and related software. The CTO is responsible for the process to manage this development. The process includes the following:
 - a. Requests for new programs or program changes are reviewed by the Product Development Manager. If approved, proposed changes are added to the Product Backlist.
 - b. A Product Roadmap is maintained by the Director of Product and is reviewed with the CEO and CTO on a regular basis.
 - c. Detailed documentation of software development and testing procedures.

- d. Documentation of approvals, development, testing results of testing, and implementation into production. This 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 with the employees who develop/test code not having access to introduce new or modified code into the production environment.
- g. All In-house developed changes to controlled regulatory processes software will be submitted for ITL approval as previously noted.

Note: For ICS #47(e) and (f) a system administrator is precluded from developing/testing code, which will be introduced into the production environment.

- h. Secured repositories for maintaining code history.
 - i. Where applicable, end-user documentation (guides and manuals).
48. Following Independent Testing Lab review and approval, an Associated Equipment form is completed and submitted to the commission for each new program or program change, and a record that such software was approved for use, is maintained.

Purchased Software Programs

Note: IT ICS #49 applies when IT personnel perform in-house modifications to a purchased software program.

49. New programs and program changes for purchased systems are documented as follows:
- a. Documentation is maintained and includes a record of software license purchase and instructions for deployment.
 - b. A copy of the associated equipment reporting form submitted to the commission 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 system manufacturer, who documents such changes and obtains necessary approvals by the Board prior to full implementation.

Data Access Control

50. 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.

Transactional information is protected via several methods. Firstly, the source data maintained by the CBS Sports System, which includes bet transaction detail records, is stored in a proprietary OpenVMS data storage technology called RMS. There currently are no direct methods to access the source data outside of the CBS Sports application. In addition, transactional and logging data stored in relational database systems, such as MySQL, are restricted and protected via network security (i.e. firewalls and VLAN segmenting) as well as user access control and logging. Only authorized IT personnel are physically able to connect to production relational database systems and that access is provided for support and infrastructure monitoring purposes only. For any Board approved cashless wagering system (including systems utilizing promotional accounts and/or wagering accounts), a method that has been approved by the chairman is utilized that renders all critical cashless wagering system stored data non-alterable. Critical cashless wagering system data includes data relating to, but not limited to, promotional account and wagering account personal identification numbers and account balances.

51. 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 related to, but not limited to, wagering instruments' validation numbers and dollar value, promotional and wagering accounts' personal identification numbers and account balances, and unpaid winning tickets information.

Critical system stored data is protected via several methods. Firstly, the source data maintained by the CBS Sports System, which includes patron wagering account personal information, is stored in a proprietary OpenVMS data storage technology called RMS. There currently are no direct methods to access the source data outside of the CBS Sports application. In addition, transactional data stored in relational database systems, such as MySQL, are restricted and protected via network security (i.e. firewalls and VLAN segmenting) as well as user access control and logging. Only authorized IT personnel are physically able to connect to production relational database systems and that access is provided for support and infrastructure monitoring purposes only.

52. Procedures are in place to ensure that any communication with equipment or programs external to the approved system is performed through a Board 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 Board approved systems by external programs. Network access is protected via segmented VLAN's and all network traffic routes through one or more firewall systems. By default, communication between two points on the network is disabled. In order to enable access, a specific "white list" rule has to be created and stored on the firewall infrastructure. The white-list rules include the TO and FROM IP Address ranges, VLAN, ports and protocols required for access. Communication from a remote sports book location includes a secure gateway setup between the remote site and the primary production data center where the CBS Sports System resides. All traffic is encrypted and secured at both ends to ensure reliability and data integrity. All traffic utilized in mobile application wagering is also encrypted via certificate pinning to ensure the mobile application is communicating properly with the mobile mid-tier services. Each session utilizes a session token

following successful login and validation of the mobile user.

Independent Laboratory Testing

An independent test laboratory will be engaged to test and certify the components of the Sports Wagering System in accordance with the technical standard within a controlled test environment, as applicable. Any of these requirements which necessitate additional operational procedures to meet the intent of the requirement shall be documented within the evaluation report and used to supplement the scope of the operational audit. The integrity and accuracy of the operation of a Sport Wagering System is highly dependent upon operational procedures, configurations, and the production environment's network infrastructure. As such, an operational audit is an essential addition to the testing and certification of a Sport Wagering System. The operational audit, outlined below, shall be performed at a frequency specified by the regulatory body:

- a) Operational Audit of Sports Wagering Procedures and Practices. This includes, but is not limited to, review of the ICS, procedures and practices for wagering operations, including, but not limited to establishing wagering rules, suspending events, handling various wagering and financial transactions, creating markets, settling wagers, closing markets, cancellations of events, voiding or cancelling wagers, player account management, fundamental practices relevant to the limitation of risks, and any other objectives established by the regulatory body.
- b) Operational Audit of Technical Security Controls. This includes, but is not limited to, an information security system (ISS) assessment, review of the operational processes that are critical to compliance, penetration testing focused on the external and internal infrastructure as well as the applications transferring, storing and/or processing of player data and/or sensitive information, and any other objectives established by the regulatory body.
- c) WHUS defines the following critical levels of our change management internally, and from a manufacturer standpoint of criticality regarding changes/updates are risk-based and typically identified as follows:

Emergency – An immediate and widespread customer outage, financial risk, and/or regulatory finding
 - For Emergency Fix's that directly relate to a specific regulatory control, we will ask for permission from the IRGC to do an immediate release and we would simultaneously start the process of sending the change to the testing lab for approval and certification

Expedited – A significant issue that cannot wait for the formal CAB approval workflow

Significant – A change that has a widespread effect on a group(s), but does not hinder the functionality of the group(s)

Major – A change with the potential of having a significant impact to the functionality of a group

Minor – A change with low risk and impact to the operation

- d) Internal Change Management, specifically changes and/or updates to controlled and non-controlled files (see note below), utilize a risk-based strategy as outlined above, which denotes an extremely high priority for the most critical updates. For example, an "Expedited" issue or change would hold priority over a "Minor" change in terms of ITL submission. Requested changes or updates to one or more controlled files have been critically determined internally by

order prior to ITL submission. To expand on this process, criticality is determined initially by the change requester and reviewed by an internal *CAB (Change Advisory Board) where criticality can be modified if necessary. Additionally, changes and updates could include but are not limited to core functionality, regulatory concerns, or issues identified on the field.

Notifications to the IRGC will be provided 5 days in advance of any critical system change or release with the exception of emergency fixes. The notification includes the following information:

- a. Description of the reasons for the proposed modification;
- b. list of the computer components and programs or versions to be replaced;
- c. description of any screens, menus, reports or operating processes that will be affected;
- d. method to be used to complete the proposed modification;
- e. date the proposed modification will be installed, and estimated time for completion;
- f. name, title and employer of the person(s) to perform the installation;
- g. diagrammatic representation of the proposed hardware design change;
- h. and any additional screen shots or visuals necessary to understand the proposed change.

Note: All changes/updates that are part of a release, both controlled and non-controlled, will be included in the part of the release notes. that are supplied 5 days prior to any release.

*** Core CAB members are leaders from various teams that review and approve change requests that may affect their areas of support or responsibility. The core CAB members are comprised of IT, Technical Compliance, Business, and subject matter experts.**