**Section 3000.661 Minimum Standards for Voucher Systems**

A Voucher System shall, at a minimum:

a) Perform the following minimum functions to control access to the System:

1) Generate daily monitoring logs of user access, security incidents and unusual transactions, and immediately notify or cause to immediately notify the Board and the MIS Department pursuant to the Owner licensee’s approved Internal Controls of critical security incidents and unusual transactions;

2) Assign rights and privileges to each user, including:

A) allowance for the secure administration of user accounts to provide an adequate separation of duties; and

B) adequate password parameters, such as lockout, minimum length, and expiration interval;

3) Use appropriate access protocols to restrict unauthorized users from viewing, changing or deleting critical files and directories;

4) Utilize encryption or password protection or equivalent security for files and directories containing critical or sensitive data. If encryption is not used, users shall be restricted from viewing the contents of such files and directories, which at a minimum shall provide for:

A) the effective segregation of duties and responsibilities with regard to the system in the MIS Department; and

B) the automatic monitoring and recording by the system of access by any person to such files and directories;

b) Perform the following minimum functions to control system operations:

1) Validate the identity of those devices from which a transmission is

received;

2) Ensure that all data sent through a transmission is completely and accurately received; and

3) Detect the presence of corrupt, or instances of lost, data and, as necessary, reject the transmission;

c) Perform the following minimum functions to control the integrity of data:

1) Generate or cause to be generated a validation number for each Voucher, either utilizing a unique algorithm, or by such other method approved by the Administrator and the certification laboratory, which method shall prevent the ability to predict the composition of any other validation number generated by the system;

2) Validate the data type and format of all inputs to critical fields and reject any corrupt data;

3) Provide for the automatic and independent recordation of critical data upon issuance of a Voucher and redemption; and

4) Provide for verification of the information contained on a Voucher presented for redemption and for the record of unredeemed Vouchers to a source that separately records and maintains transaction data, or such other compensating procedure as approved by the Administrator and the certification laboratory, which procedure shall independently verify the accuracy of the validation number and value prior to redeeming the Voucher;

d) Perform the following minimum functions to address business continuity:

1) Utilize data redundancy techniques that ensure system data preservation;

2) Utilize environmental controls, such as uninterruptible power supplies, and fireproof and waterproof materials to protect critical data from natural disaster; and

3) Immediately notify or cause to immediately notify the Board pursuant to the Owner licensee’s approved Internal Controls and MIS of any malfunction that threatens the integrity of the Voucher System;

e) Insure that the Voucher System is not capable of issuing or validating a duplicate Voucher on demand;

f) Insure that if the validation information cannot be sent to the Voucher System, an alternate method of payment is provided:

1) By the Voucher System possessing unique features to identify duplicate

Vouchers and prevent fraud by redeeming an unexpired and/or unvalidated Voucher that was previously issued by the EGD; or

2) Pursuant to the Owner licensee’s approved Internal Controls;

g) Insure that once the validation information is stored in the database, the data may not be altered in any way;

h) Insure that any device that holds Voucher information in its memory shall not allow removal of the information unless it has first transferred that information to the database or other secured components of the Voucher System;

i) Insure that only designated Vouchers can be issued and redeemed;

j) Insure that each Voucher System is designed and is operated so as to prevent the use of counterfeit Vouchers, previously redeemed Vouchers, incomplete Vouchers if the validation information is missing, expired Vouchers, or Vouchers issued at other Riverboat Gaming Operations and by other holders of an Owner's license;

k) Insure that remote access is prohibited unless the Administrator has approved internal controls that specifically address remote access procedures;

l) Insure that all Voucher transactions are retained for the prior three years, either on-line or in a media approved by the Administrator and capable of being restored to the Voucher System upon request; and

m) Insure that Electronic Credits from a Voucher that are not evenly divisible by the minimum wager amount of an Electronic Gaming Device, including the accumulation of fractional amounts from multiple vouchers, are issued to the patron in a Voucher for the full value of the fractional Electronic Credit.

(Source: Amended at 32 Ill. Reg. 17946, effective November 5, 2008)