AMENDMENT TO CONTRACT

This agreement is entered into as of the 26 day of June 2005 (the "Effective Date"), in relation to the GMIS registration forms by and between Utah Interactive ("Portal Operating Company" or "POC") and GMIS-Utah.

WITNESSETH:

WHEREAS, POC and Entity desire to include provisions mandated by the current requirements of the Payment Card Industry's Data Security Standards ("the DSS").

NOW, THEREFORE, POC AND ENTITY agree to the following:

1. **Definitions.**

   a. "Acquirer" means a Member that initiates and maintains relationships with merchants that accept Visa or MasterCard cards.

   b. "Cardholder Data" means all personally identifiable data about the cardholder and relationship to the Member (i.e., account number, expiration date, data provided by the member, other electronic data gathered by the merchant/agent, magnetic stripe data, etc.). This term also accounts for other personal insights gathered about the cardholder, i.e., addresses, telephone numbers, etc..

   c. "CVC2/CVV2" means the three-digit value printed on the signature panel of a payment card used to verify card-not-present transactions. On a MasterCard payment card this is called CVC2. On a Visa payment card this is called CVV2.

   d. "Encryption" means the process of converting information into a form unintelligible to anyone except holders of a specific cryptographic key. Use of encryption protects information against unauthorized disclosure between the encryption process and the decryption process (the inverse of encryption).

   e. "Encryption key" means a value applied using an algorithm to unencrypted text to produce encrypted text.

   f. "Magnetic stripe data" means data encoded in the magnetic stripe on a payment card that is used for authorization during a card-present transaction.

   g. "Member" means a member of a bankcard association, such as a Bank or Credit Union, through which a MasterCard, Visa or Discover payment card is issued.

h. "Merchant" means POC as it stores, transmits or processes cardholder data for purposes of performing its obligations to complete portal users' payments for authorized transactions under the Contract.

i. "Sensitive cardholder data" means data whose unauthorized disclosure may be used to facilitate a fraudulent transaction. It includes the account number, magnetic stripe data, CVC2/CVV2 and expiration date.

2. **PURPOSE OF THIS AGREEMENT**. The purpose of this Agreement is to address requirements mandated by the DSS and thus include the following provisions:

a. If the Entity has access to cardholder data, it agrees it will adhere to the requirements of the DSS.
b. If the Entity has access to cardholder data, the Entity acknowledges it is responsible for security of the cardholder data in its possession, in accordance with the DSS.
c. Entity acknowledges that ownership of cardholder data resides with either Payment Card brand, Acquirer, or Merchant, but does not reside with Entity. Entity further acknowledges that such data can ONLY be used by Entity for assisting the Payment Card brand, the Acquirer or Merchant in completing a transaction, supporting a loyalty program, providing fraud control services, or for others uses specifically required by law.
d. Entity agrees that it will provide business continuity for its operations that involve Cardholder data, in the event of a major disruption, disaster or failure.
e. In the event of a security intrusion involving Entity, Entity agrees that any Payment Card Industry representative, or a Payment Card Industry approved third party, or POC or a designated representative of POC, will be provided with full cooperation and access by Entity, as they seek to conduct a thorough security review, including a review of Agency's operations involving Cardholder data. . The purpose of the review will be to validate compliance with the DSS for protecting Cardholder data.
f. Entity agrees to continue to treat Cardholder data as confidential following termination of the Contract until it is properly destroyed following the required retention period.
g. Entity agrees that if Entity is permitted or required to store Sensitive Cardholder data under this Contract, it must render the Sensitive Cardholder data unreadable by encryption anywhere it is stored (including data on portable media, backup media, in logs, and data received from or stored by wireless networks).
h. Entity further agrees that if Entity has Encryption Keys, it must protect them against both disclosure and misuse by (1) restricting access to keys to the fewest number of custodians necessary; and (2) by storing keys securely in the fewest possible locations and forms, and (3) in accordance with security practices that meet or exceed industry standard.

3. In the event that future data security standards or procedures in addition to those in this Agreement are promulgated and required or recommended by the Payment Card Industry, the parties agree that such further and future data security standards or procedures may be incorporated into this Agreement by a letter of notification from POC or one of its affiliated companies, to Entity, upon which Entity will be required to note, by signature of an authorized agent upon such letter returned to POC, its acknowledgement and agreement to such further data security standards or procedures.

IN WITNESS WHEREOF, POC and Entity have caused this Agreement to be signed and delivered by their duly authorized representatives as of the date first set forth above.

"ENTITY"	**"POC NAME""**
Signed B. Brown	Carrie Gott
Print Name Brad Brown	CARRIE GOTT
Title DABC IT Director	General Manager
Date April 24, 2006	April 24, 2006