GLO Information Security Appendix

1. Definitions

"Breach of Security" or "Breach" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information including data that is encrypted if the person accessing the data has the key required to decrypt the data.

"GLO Data" means any data or information owned by the GLO, including PII or SPI as defined below, that Provider creates, obtains, accesses (via records, systems, or otherwise), receives (from the GLO or on behalf of the GLO), or uses in the course of Contract performance.

"Personal Identifying Information" or "PII" means information that alone, or in conjunction with other information, identifies an individual as defined at Tex. Bus. & Com Code 521.002(1).

"Sensitive Personal Information" or "SPI" means the information categories listed at Tex. Bus. & Com Code 521.002(2).

2. Security and Privacy Compliance

2.1. Provider shall keep all and GLO Data received under the Contract strictly confidential.

2.2. Provider shall comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations.

2.3. Provider shall implement administrative, physical, and technical safeguards to protect GLO Data that are no less rigorous than accepted industry practices including, without limitation, the NIST Cybersecurity Framework. All such safeguards shall comply with applicable data protection and privacy laws.

2.4. Provider will legally bind any subcontractors to the same requirements stated herein and obligations stipulated in Provider's contract with the GLO. Provider shall ensure that the requirements stated herein are imposed on any subcontractor of Provider's subcontractor(s).

2.5. Provider will not share GLO Data with any third parties.

2.6. Provider will ensure that initial privacy and security training, and annual training thereafter, is completed by its employees or subcontractors that have access to GLO Data or who create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally handle PII on behalf of the agency. Provider agrees to maintain and, upon request, provide documentation of training completion.

2.7. Any GLO Data maintained or stored by Provider or any subcontract must be stored on servers or other hardware located within the physical borders of the United States and shall not be accessed outside of the United States.

3. Data Ownership

3.1. GLO shall retain full ownership of all respective data provided to Provider or to which the Provider otherwise gains access by operation of the Contract.

3.2. Upon termination of the Contract, Provider shall promptly return to the GLO all GLO Data possessed by Provider and its agents or subcontractors. Provider shall retain no copies or back-up records of GLO Data. If such return is infeasible, as mutually determined by the GLO and Provider, the obligations set forth in this **Attachment**, with respect to GLO Data, shall survive termination of the Contract and Provider shall limit any further use and disclosure of GLO Data to the purposes that make the return of GLO Data infeasible. In lieu of the requirements in this Section 3.2, the GLO may direct Provider to destroy any GLO Data in Provider's possession. Any such destruction shall be verified by Provider and the GLO.

4. Data Mining

4.1. Provider agrees not to use GLO Data for unrelated commercial purposes, advertising or advertising-related services, or for any other purpose not explicitly authorized by the GLO in this Contract.

4.2. Provider agrees to take all reasonably feasible, physical, technical, administrative, and procedural measures to ensure that no unauthorized use of GLO Data occurs.

5. Breach of Security

5.1. Provider agrees to provide the GLO with the name and contact information for an employee of the Provider which shall serve as the GLO's primary security contact.

5.2. Upon discovery of a Breach of Security or suspected Breach of Security by the Provider, the Provider agrees to notify the GLO as soon as possible, but in no event longer than 24 hours, upon discovery of the Breach of Security or suspected Breach of Security. Within 72 hours, the Provider agrees to provide, at minimum, a written preliminary report to the GLO with root cause analysis including the total number of records affected.

5.3. The initial notification and report shall be submitted to the GLO Information Security Officer at informationsecurity@glo.texas.gov.

5.4. Provider agrees to take all reasonable steps to immediately remedy a Breach of Security and prevent any further Breach of Security.

5.5. Provider agrees that it shall not inform any third party of any Breach of Security or suspected Breach of Security without first obtaining GLO's prior written consent.

5.6. If the Breach of Security includes SPI, including Social Security Numbers, payment card information, or health information, the Provider agrees to provide affected individuals complimentary access for one (1) year of credit monitoring services.

6. Right to Audit

6.1. Upon the GLO's request and to confirm Provider's compliance with this **Attachment**, Provider grants the GLO, or a GLO-contracted vendor, permission to perform an assessment, audit, examination, investigation, or review of all controls in the Provider's, or Provider's subcontractor's, physical and/or technical environment in relation to GLO Data. Provider agrees to fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure and

application software that stores, processes, or transports GLO Data. In lieu of a GLO-conducted assessment, audit, examination, investigation, or review, Provider may supply, upon GLO approval, the following reports: SSAE18, ISO/ICE 27001 Certification, FedRAMP Certification, PCI Compliance Report. Provider shall ensure that this clause concerning the GLO's authority to assess, audit, examine, investigate, or review, is included in any subcontract it awards.

6.2. At the GLO's request, Provider agrees to promptly and accurately complete a written information security questionnaire provided by the GLO regarding Provider's business practices and information technology environment in relation to GLO Data.