Trustwell

Exhibit A Security Controls

1.1. Trustwell will only use Client Data for the purposes of fulfilling its obligations under the Agreement. Trustwell will maintain and enforce physical and logical security procedures with respect to its access and maintenance of Client Data contained on Trustwell servers.

1.2. Trustwell will use reasonable measures to secure and defend its location and equipment against "hackers" and others who may seek to modify or access the Trustwell servers or the information found therein without authorization. Trustwell will test its systems for potential security breaches at least annually.

1.3. Trustwell has a written information security program ("Information Security Program") that includes administrative, technical, and physical safeguards that protect against any reasonably anticipated threats or hazards to the confidentiality of the Client Data, and protect against unauthorized access, use, disclosure, alteration, or destruction of the Client Data. In particular, Truswell's Information Security Program shall include, but not be limited, to the following safeguards where appropriate or necessary to ensure the protection of Confidential Information and Client Data:

1.3.1. Access Controls – policies, procedures, and physical and technical controls: (i) to limit physical access to its information systems and the facility or facilities in which they are housed to properly authorized persons and (ii) to authenticate and permit access only to authorized individuals.

1.3.2. Security Incident Procedures – policies and procedures to detect, respond to, and otherwise address security incidents, including procedures to monitor systems and to detect actual and attempted attacks on or intrusions into Client Data or information systems relating thereto, and procedures to identify and respond to validated security incidents, mitigate harmful effects of security incidents, and document security incidents and their outcomes.

1.3.3. Contingency Planning – policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages Client Data or systems that contain Client Data, including a data backup plan and a disaster recovery plan.

1.3.4. Device and Media Controls – policies and procedures that govern the receipt and removal of hardware and electronic media that contain Client Data into and out of a Trustwell data center, and the movement of these items within a Trustwell data center, including policies and procedures to address the final disposition Client Data.

1.3.5. Audit controls – hardware, software, and/or procedural mechanisms that record activity in information systems that contain or use Client Data.

1.3.6. Data Integrity – policies and procedures to guard against the unauthorized disclosure, improper alteration, or unauthorized destruction of Client Data.

1.3.7. Transmission Security – encryption of Client Data at rest within the SaaS Applications and encryption of electronic information while in transit to guard against unauthorized access to Client Data that is being transmitted over public communications network.

1.3.8. Secure Disposal – policies and procedures regarding the disposal of Client Data, taking into account available technology that can be used to sanitize storage media such that stored data cannot be practicably read or reconstructed.

1.3.9. Testing – Trustwell shall regularly test the key controls, systems and procedures of its Information Security Program to verify that they are properly implemented and effective in addressing the threats and risks identified. Tests will be conducted or reviewed in accordance with recognized industry standards (e.g., AICPA, SSAE 18, and their successor audit standards, or similar industry recognized security audit standards).

1.3.10. Adjust the Program – Trustwell shall monitor, evaluate, and adjust, as it deems necessary, the Information Security Program in light of any relevant changes in technology or industry security standards, the sensitivity of Client Data, and internal or external threats to Trustwell or the Client Data.

1.3.11. Security Training – Trustwell shall provide annual security awareness and data privacy training for its employees that will have access to Client Data.

1.3.12. Confidentiality - Trustwell shall require that all Trustwell employees who are granted access to Client Data undergo appropriate screening, where lawfully permitted, and enter into a confidentiality agreement prior to being granted such access.