GEORGIA TECH SERVICE PROVIDER PCI DSS WRITTEN AGREEMENT

1. For the purposes of this section, the following terms will have the meaning ascribed to them herein.

a. “Applications” includes, but is not limited to, all purchased and custom external (web) applications;

b. “Cardholder Data” shall mean any personally identifiable data associated with a cardholder, including, by way of example and without limitation, a cardholder’s account number, expiration date, name, address, social security number, or telephone number;

c. “Network Components” includes, but is not limited to, Provider’s firewalls, switches, routers, wireless access points, network appliances, and other security appliances;

d. “Servers” includes, but is not limited to, all of Provider’s web, database, authentication, DNS, mail, proxy and NTP servers;

e. “Subcontractors” means all parties, if any with which Provider contracts, directly or indirectly, in order to perform its obligations under the Agreement.

f. “Institute” means the Georgia Institute of Technology (Georgia Tech).

2. Provider agrees, on behalf of itself and each of its Subcontractors, that it shall be responsible for the security of any cardholder data possessed or otherwise stored, processed or transmitted on behalf of the customer, or to the extent that Provider could impact the security of the customer’s cardholder data environment. Provider shall use Cardholder Data (CHD) only for assisting cardholders in completing a transaction, supporting a loyalty card program, providing fraud control services, or for other uses specifically required by law.

3. Provider represents and warrants that all of its Network Components, Applications, Servers, and Subcontractors comply with the current version of the Payment Card Industry Data Security Standard (“PCI DSS”), and any successors thereto. Provider will immediately notify Georgia Tech Cyber Security by sending an e-mail to compliance@security.gatech.edu if Provider learns that it or any of its subcontractors are no longer PCI DSS compliant and will immediately provide the Institute the steps being taken to remediate the non-compliant status. In no event shall Provider’s notification to the Institute be later than seven (7) calendar days after Provider learns of the non-compliant condition.

4. Provider shall have a business continuity program which conforms to PCI DSS to protect Cardholder Data (CHD) in the event of a major disruption in its operations or in the event of any other disaster or system failure which may occur to Provider’s operations.

5. Provider, for itself and all subcontractors, agrees (a) to provide Institute a copy of a mutually acceptable PCI DSS compliance document containing information about which PCI DSS requirements are managed by the provider; (b) that Institute will have the right to review the audit criteria for any such documentation, and agrees to use commercially reasonable efforts to incorporate any audit criteria recommended by Institute into the actual audit criteria use; (c) that the documentation will be updated and a copy provided to Institute annually; (d) that it will notify the Institute at least 60 days prior to any substantial change to the processing environment that may impact the Institute; (e) that it will establish and maintain all application and system logs under its domain and further agrees to provide to Institute a copy of all logs if so requested; and (f) that such facilities are in compliance with relevant Institute security policies.

6. In the event of a breach or intrusion, or otherwise unauthorized access to cardholder data stored at or for Provider, Provider shall immediately notify Georgia Tech Cyber Security by calling (404) 385-CYBR (2927) or sending an e-mail to soc@gatech.edu stating that this incident involves cardholder data. This will allow the proper PCI DSS compliant breach notification process to commence. Provider shall provide appropriate payment card companies, acquiring financial institutions, and their respective designee's access to the Provider's facilities and all pertinent records to conduct a review of the Provider's compliance with the PCI DSS requirements. Provider will cooperate with representatives or agents of the payment card industry and/or Institute in conducting a thorough security review of Provider's operations, systems, records, procedures, rules and practices in the event of a security intrusion in order to validate Provider's compliance with PCI DSS.

7. Provider shall respond in a timely manner and fully to those portions of the PCI DSS Annual Self-Assessment Questionnaire or any other documentation demonstrating compliance sent to it by the Institute.

8. Provider shall continue to safeguard Cardholder Data in the event this Agreement terminates or expires.

Service Provider Name Date