DATA SECURITY SCHEDULE

1. **Personal Data.** "Personal Data" shall mean any information related to any identified or identifiable natural or legal person, such as end users of Client websites, Client's employees, subcontractors or any third party and any other additional information deemed as personal data under applicable data protection laws, which is available to Monetate for processing on behalf of Client pursuant to the Agreement.

2. **Compliance with Privacy Laws.** Client is the controller of Personal Data relating to such Client and its respective subsidiaries, divisions, Affiliates, employees, or customers for the purposes of applicable privacy laws, with rights to determine the purposes for which the Personal Data is processed. Nothing in the Agreement will restrict or limit Client's rights or obligations as owner and controller of Personal Data for such purposes. Monetate is a processor or service provider of the Personal Data for purposes of applicable privacy laws. As controller of the Personal Data, Client is directing Monetate to process the Personal Data in accordance with the terms of this Agreement. Client hereby represents and warrants that its privacy policy shall comply with all relevant privacy laws in all jurisdictions in which it employs the Web Services.

3. **Credit Card Storage.** As required, Monetate shall collect credit card information as part of the completion to an e-commerce transaction. Monetate shall encrypt such information within its system for the sole purpose of handing the encrypted information to Client's designated payment gateway. Monetate shall not be required to process, store or otherwise handle credit card information except within its designation as a PCI third party service provider. To the extent that Monetate is required to store any credit card information (or encrypted information that may contain credit information), Monetate shall purge such information within a commercially reasonable amount of time.

4. **PCI Compliance.** Monetate shall comply with the Payment Card Industry's ("PCI") rules and regulations, including but not limited to the data security standards, including (i) providing data security reports as may be required by the credit card issuer; (ii) paying any fines and penalties in the event Monetate fails to comply with such data security requirements; and (iii) fully cooperating with, and providing access to, the credit card issuer or credit card association to conduct a security review of Monetate's policies and procedures. A failure by Monetate to cure any non-compliance with the PCI rules and regulations shall be deemed a material breach by Monetate of the Agreement. Monetate shall at its own expense undergo a PCI compliance audit on no less than an annual basis and, upon request, provide the attestation of the results of such audit to Client.

5. **Processing of Personal Data**
    a. Monetate may process the Personal Data only to perform its obligations under the Agreement and may disclose the Personal Data only to Monetate employees that have a need to know for the performance of such obligations, have received privacy training from Monetate, and are bound by confidentiality obligations not less restrictive than those contained in the Agreement. Monetate may not sell, rent or lease Personal Data.
    b. In cases where Monetate subcontracts services involving collecting, using, storing, transferring and otherwise processing Personal Data, Monetate will require its subcontractors to protect and process the Personal Data under terms no less restrictive than those contained in this Data Security Schedule. Furthermore, Client reserves the right, at its sole option, to enter into additional confidentiality agreements directly with such subcontractors in order to ensure adequate protection of the Personal Data and comply with any applicable privacy laws.

6. **Security Measures.** Monetate shall use the same degree of care, but never less than a reasonable degree of care, to prevent unauthorized use, dissemination or publication of the Personal Data, as it uses to protect its own information of a similar nature, and will implement any technical and organizational measures to protect the Personal Data which are required by the applicable law. At a minimum, Monetate agrees:

    a. To implement appropriate technical and organizational measures to protect the Personal Data against (i) accidental or unlawful destruction or loss, (ii) unauthorized disclosure or access, in particular where processing involves the transmission of the Personal Data over a network, (iii) alteration, and (iv) all other unlawful forms of processing.
    b. To implement appropriate procedures to ensure that (i) unauthorized persons will not have access to the data processing equipment used to process the Personal Data, (ii) any persons it authorizes to have access

to the Personal Data will respect and maintain the confidentiality and security of the Personal Data, and (iii) the measures and procedures that it uses will be sufficient to comply with all applicable legal requirements.

7. **DDOS (Distributed Denial-Of-Service) Protection.** Monetate shall monitor the Web Services to proactively attempt to mitigate the effect of a DDOS attack. At all times, Monetate shall maintain and update standard operating procedures on handling, addressing and resolving potential DDOS attacks. To the extent that Monetate detects a DDOS attack on the Web Services, Monetate shall take all commercially reasonable steps in order to immediately mitigate the effect of the attack, which may include, but will not be limited to, a) filtering site traffic to a separate instance of the site based on the source of the intrusion, and b) increasing the sensitivity of all firewalls and security networks in order to preserve traffic. Monetate may take commercially reasonable steps necessary to mitigate the effect of a DDOS attack immediately and without Client's permission.

8. **Additional Monetate Obligations.**
    a. Monetate will only process Personal Data in accordance with the requirements of the Agreement, for the purpose of providing the Web Services contemplated under the Agreement.
    b. Monetate will immediately notify Client if it becomes aware of any unauthorized use of, disclosure of, or access to the Personal Data by itself or others, including notification of loss of data whether or not such data has been encrypted.
    c. Monetate will cooperate with Client in the manner reasonably requested by Client and in accordance with law, including but not limited to: conducting the investigation; cooperating with authorities; notifying affected persons, credit bureaus, other persons or entities deemed appropriate by Client; and issuing press releases. Such cooperation will include: (1) Client access to relevant Monetate records and facilities; (2) Monetate provision of all relevant data and reports to Client; and (3) timely advance approval by Client of any notifications to impacted individuals or press releases.
    d. Monetate will promptly inform Client in writing if Monetate is of the opinion that any instruction from Client violates applicable data protection laws.
    e. When collecting, using, storing, transferring and otherwise processing, Monetate shall adhere to applicable data protection laws.

9. **Records**
    a. Monetate is bound by the provisions of the Agreement to protect the security and confidentiality of the Personal Data collected from its clients. In order to ensure that Client's Personal Data is being adequately protected Client may request relevant compliance documentation from Monetate for facilities and security practices that are under Monetate's direct control, including 1) PCI Attestation of Compliance and 2) SOC 1, SOC 2, and/or SOC 3 Reports. However, Monetate will not provide detailed reports that disclose information regarding other clients.
    b. Monetate utilizes a shared responsibility model with Amazon Web Services ("AWS"). Due to non-disclosure obligations with AWS, Monetate may be unable to provide certain security documentation directly to Client. However, Client may request security documentation directly from AWS, including, but not limited to: 1) the AWS PCI Compliance Package, and 2) AWS SOC 2 Report.