Schedule D to the Spirion Software as a Service Agreement

Data Privacy and Security Policy

1. Information Security. Spirion will use commercially reasonable efforts to maintain the security, integrity and availability of all Customer Data received from Customer, including but not limited to commercially reasonable efforts reflecting changing technological approaches, to comply with the following measures with respect to Customer Data:

1.1 maintain commercially customary physical security and access controls;
1.2 maintain commercially customary network security controls including firewall and intrusion prevention solutions;
1.3 maintain commercially customary redundancy at the demark, network and system layers;
1.4 maintain commercially customary monitoring solutions to continually manage health and capacity of the IT infrastructure of the System;
1.5 provide data encryption in a commercially customary manner of all data transmissions;
1.6 require individual user accounts and passwords for any access;
1.7 maintain generally acceptable user account management processes and procedures;
1.8 maintain industry accepted data protection program;
1.9 maintain and periodically test (at least annually) a commercially customary disaster recovery plan that provides adequate system backup, technology replacement, and alternate (backup-site) site capabilities;
1.10 follow commercially customary hardening procedures for system/device builds;
1.11 conduct ongoing vulnerability management through the use of commercially customary tools; and
1.12 follow commercially customary change and release management practices for hardware and software changes.

2. Privacy. Spirion will comply with all applicable laws regarding the privacy of consumer information. If Spirion will process Personal Data under the Agreement: (a) it shall process Personal Data (a) only on behalf of and for the benefit of Customer in connection with the Services under the Agreement; (b) in strict compliance with applicable laws and with any applicable Data Processing Agreements, which shall be attached hereto. Spirion agrees that the parties may add additional data privacy agreements or addenda as attachments in the event that additional laws become applicable.

3. Data Security Incident Response

If Spirion becomes aware of a confirmed breach of the security measures described in this Spirion Data Privacy and Security Policy that results in either (a) unlawful access to Customer Data stored on Spirion's equipment or in Spirion's facilities, or (b) unauthorized access to such equipment or facilities, where in either case such access results in loss, disclosure, or alteration of Customer Data (each a "Security Event"), Spirion will: (x) notify Customer of the Security Event using the email address listed in Customer's Spirion account within 24 hours after Spirion confirms the Security Event (provided Spirion is not prohibited from providing the notification by a court order or other legal requirement); and (y) promptly take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Event. Spirion shall assist the Customer, where required by applicable law, to notify any Security Event to the competent government entity and to affected individuals.

4. Insurance

Spirion will maintain insurance covering impacts directly related to cyber security incidents involving Services supplied under the Agreement.

***