MOSAIC DATA SYSTEMS SECURITY EXHIBIT

This Mosaic Data Systems Security Exhibit ("**Security Exhibit**") shall be incorporated into the Master Agreement between the parties, including all Work Orders initiated thereunder. The requirements contained herein are in addition to those outlined in the Master Agreement and any Work Order attached thereto.

Definitions

"Authorized Contractor Employees" is defined as those employees who are authorized to access Mosaic's computer network or systems. Contractor shall provide to Mosaic a written list of the names, titles and location of Contractor's employees that Contractor is requesting should have access to Mosaic's computer network or systems. Mosaic shall have the opportunity to review and approve the listing of Authorized Contractor Employees. Contractor shall be solely responsible for ensuring that Authorized Contractor Employees are not security risks.

"**Availability**" is defined as remaining available for use by Mosaic in the normal course of business, availability includes Mosaic Data, the associated storage devices, along with the associated hardware and software used to secure, access, or process Mosaic Data along with the associated communications channels managed by Contractor in support of services provided to Mosaic.

"**Confidentiality**" is as defined in the Master Agreement. In the absence of such definition in the Master Agreement, Confidentiality is defined as maintaining controls over Mosaic Data in a manner that strictly enforces a "Need to Know" level of access. The "Need to Know" must be based upon a defined business need and include actions required to be performed by or on behalf of Mosaic directly related to Mosaic business processes or in direct support of the services provided by Contractor to Mosaic.

"**Integrity**" is defined as the completeness and accuracy of Mosaic Data as entered, modified or updated in the Contractor environment.

"**Least Privilege**" is defined as providing the lowest level of access privileges (read, write, modify, delete, etc.) to Mosaic Data required in order to fulfill daily responsibilities necessary to act on behalf Mosaic or in support of services provided to Mosaic by Contractor.

1. **Security Program.** During the term of the Master Agreement, Contractor shall maintain and implement a formal security program in accordance with industry standards (the "**Security Program**") that is designed to (i) ensure the security, Confidentiality and Integrity of Mosaic's data or information ("**Mosaic Data**") developed, received, accessed, or acquired by Contractor in performance of the services and all derivatives thereof, (ii) protect against threats or hazards to the security, Confidentiality and Integrity of Mosaic Data; and (iii) prevent unauthorized access to or intentional or accidental destruction, loss, alteration, or unauthorized disclosure of Mosaic Data. Without limiting the scope of this Security Exhibit or the Master Agreement, Contractor shall require its employees, agents, representatives, subcontractors, and any other party engaged by Contractor in support of the services provided to Mosaic ("**Contractor Personnel**") to agree in writing to be bound by security terms no less restrictive than those contained in the Master Agreement, and Contractor shall be liable for the compliance of such Contractor Parties. The Security Program applies to the business computing environment of Contractor and the Contractor Parties in which Mosaic Data is stored, accessed or otherwise processed. At all times Contractor shall comply with applicable data privacy laws and regulations.

2. **Unauthorized Disclosure.** Contractor shall not disclose Mosaic Data for any purpose other than what is necessary to fulfill the purpose of and in accordance with the Master Agreement. If Contractor or Contractor Parties believes that there has been a disclosure of Mosaic Data to anyone other than Contractor or Contractor Parties, such party must promptly notify Mosaic and comply with all Security Breach remediation efforts contained in the Master Agreement.

3. **Mosaic Data Storage.** Subject to the terms of this provision, Mosaic Data will be housed in a data center located in the United States or Canada. Contractor represents and warrants that Mosaic Data shall not at any time during the term of the Master Agreement, be accessed, transmitted, or temporarily stored by Contractor or its affiliates or subcontractors outside the United States and Canada. Contractor shall encrypt in accordance with industry standards, or take other such reasonable security measures, to protect Mosaic Data in accordance with this Security Exhibit. Contractor will (i) comply with applicable laws related to the security and processing of Mosaic Data, and (ii) will reasonably cooperate with Mosaic in its compliance with applicable law.

4. **Logical Access Controls.** Access to Mosaic Data by Contractor in support of the services provided to Mosaic by Contractor shall remain restricted on a "Need to Know" basis. When required, access will be granted based on the Least Privilege necessary to perform required business function on behalf of or in support of services provided by Contractor. At no time shall Mosaic Data be accessible by or available to any third party except where explicit written consent is provided to Contractor by Mosaic prior to said access. Contractor shall maintain logical access controls no less than industry standard for the nature of the services provided by Contractor and appropriate for the legal requirements for the protection of Mosaic Data hosted, maintained, processed or otherwise accessed by Contractor and Contractor Parties.

5. **Physical Access Controls.** Physical access controls shall be employed to restrict physical access to the hardware that accesses or stores Mosaic Data to authorized Contractor and Contractor Party personnel who have a legitimate business need for such access. Contractor shall maintain physical access controls in the same manner which it maintains physical access controls with regard to its own information, but in no event shall such physical access controls be less than industry standard for the nature of services provided by Contractor to Mosaic.

6. **Threat Management and Security Event Monitoring.** Contractor shall monitor security trends to maintain appropriate awareness of existing and emerging threats to the Confidentiality, Integrity and Availability of Mosaic Data. Contractor shall incorporate information related to threats both current and emerging into the Security Program to actively manage and minimize the risk to Mosaic Data. Contractor shall actively monitor the Contractor business computing environments for indicators of security events that could place the Confidentiality, Integrity or Availability of Mosaic Data at risk. Security event monitoring will operate in a manner that provides immediate notification of a data security breach, whether actual or potential.

7. **Information Protection.** Only Authorized Contractor Employees using Contractor-supplied equipment may access Mosaic's computer network or systems. Contractor shall use only Mosaic approved remote network access technology to access Mosaic's computer network or systems. Mosaic retains sole discretion on remote access technology and will provide Contractor with thirty (30) days advance notice of changes to the remote access technology requirements. Prior to accessing Mosaic's computer network or systems, Contractor shall ensure all Contractor Parties are aware of and are prepared to comply with Mosaic's Acceptable Use Policy and Code of Business Conduct and Ethics. While connected to or using Mosaic's computer network and systems, Contractor shall not engage in any activity intended to disable or circumvent the security controls implemented by Mosaic. Mosaic Data used and/or created throughout the term of the Master Agreement by Contractor shall remain with the Mosaic systems and network and shall not be stored on Contractor equipment or other non-Mosaic data storage devices unless otherwise explicitly agreed upon in writing prior to Mosaic Data leaving the Mosaic systems and/or network. Contractor will promptly notify Mosaic whenever any of the Authorized Contractor Employees leave Contractor's employ or no longer require access to Mosaic's computer network or systems. Additionally, Contractor shall comply with the following requirements:

i. Contractor must have policies and procedures in place to ensure that industry standard commercial anti-virus software is installed and kept up to date on all Contractor equipment that is used to access Mosaic network or systems;
ii. Contractor must have policies and procedures in place to ensure that the latest security patches are applied in a timely manner to all Contractor equipment that is used to access Mosaic's network or systems;
iii. Contractor must use an industry standard commercial email filtering and anti-virus application; and
iv. Contractor must use an industry standard commercial web filtering software.

8. **Processing of Personal Information.** Contractor represents and warrants that it adheres to industry standard data privacy principles when collecting and processing Personal Information. Such principles include, but are not limited to:

i. Contractor collects and uses Personal Information lawfully and only for the specified purposes identified the Contract Documents;

ii. Contractor limits its collection of Personal Information to what is adequate, relevant, and necessary for its performance under the Contract Documents;

iii. Contractor shall provide Mosaic notice regarding its Personal Information processing practices in a clear and transparent matter, and shall provide Mosaic subsequent notice if those processing practices materially change during the Term;

iv. Contractor retains Personal Information for only as long as required to perform under the Contract Documents and as permitted by the Master Agreement;

v. Contractor respect the rights of the individuals whose Personal Information Contractor holds; and

vi. Contractor properly secures the Personal Information it holds and does not transfer it to any unsecured devices or third parties except as authorized by the Contract Documents.

9. **Oversight of Security Compliance.** Upon Mosaic's request, to confirm Contractor's compliance with this Security Exhibit, as well as any applicable laws, regulations, and industry standards, Contractor grants Mosaic or, upon Mosaic's election, a third party on Mosaic's behalf, permission to perform an assessment, audit, examination, or review of all controls in Contractor's physical and/or technical environment in relation to all Personal Information being handled and/or services being provided to Mosaic pursuant to the Master Agreement. Contractor shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that processes, stores, or transports Personal Information for Customer pursuant to this Agreement. In addition, upon Mosaic's request, Contractor shall provide Mosaic with the results of any audit by or on behalf of Contractor performed that assesses the effectiveness of Contractor's information security program as relevant to the security and confidentiality of Mosaic Data shared during the course of this Master Agreement.