RFgen Data Security Policy

For the service procured on the applicable Order (the "**RFgen Service**"), the DataMAX Software Group, Inc, a California corporation dba RFgen Software, located at 1101 Investment Blvd, Suite 250, El Dorado Hills, CA 95762 USA, hereafter ("**RFgen**"), shall maintain commercially reasonable administrative Safeguards designed for the protection, confidentiality, and integrity of Customer Data. All such Safeguards shall be commensurate with the importance of the Customer Data being protected, but in no event less protective than safeguards that RFgen uses to protect its own information or data of similar importance, or as required by applicable law. As of the effective date of the applicable Order Form, such Safeguards are described below in this Addendum; provided, however, that Customer acknowledges and agrees that such Safeguards described in this Addendum are not comprehensive and such Safeguards may change during the term of the applicable Order, as applicable third party security audits, compliance standards and/or certifications evolve/change over time, provided that any such changes to Safeguards will not materially decrease the overall security of the RFgen Service during the term of the applicable Order. For the term of the Agreement, RFgen shall comply with all obligations regarding Customer Data under the applicable Order, including, without limitation, RFgen's obligations to maintain commercially reasonable Safeguards as provided herein.

1. DEFINITIONS.

"Personal Information" shall have the same meaning as the term "**personal data**", "**personally identifiable information**" or the equivalent term under Applicable Data Protection Law.

"Primary DC" shall mean the primary data center in which Customer Data is stored.

"Safeguards" shall mean physical and technical safeguards.

"Security Incidents" shall mean an actual unauthorized disclosure, or reasonable belief that there has been an unauthorized disclosure, by RFgen of Customer Data containing unencrypted information to any unauthorized person or entity.

2. SECURITY POLICY.

RFgen has, and will maintain, a security policy for its security organization that requires security training and privacy training as part of the general onboarding and recurring training programs for RFgen security personnel. As part of RFgen's security policy, RFgen has, and will maintain, dedicated security personnel responsible for the ongoing monitoring of RFgen's security infrastructure, including the review of RFgen products and services, and for responding to security incidents.

3. CUSTOMER DATA CONTROLS.

RFgen has, and will maintain, measures to ensure Customer Data is processed only in accordance with the instructions provided by the Customer.

4. DATA STORAGE AND HANDLING.

Any equipment with storage capability, including mobile media, used to store Customer Data will be secured in accordance with industry standard practices. RFgen will maintain a reasonable asset management policy to manage the life cycle (commissioning, operating, maintaining, repairing, modifying, replacing and decommissioning/disposal) of such media. Decommissioned media containing Customer Data will be destroyed in accordance with NIST 800-88 Revision 2 at the Moderate level of sensitivity (or similar data destruction standard). Any Customer Data stored in RFgen managed environments will be logically segmented from RFgen and other RFgen customers' data.

5. USERS: PASSWORDS, ACCESS, AND NOTIFICATION.

Customer shall authorize access to and assign unique passwords and user names to its Users. Customer will be responsible for the confidentiality and use of User's passwords and user names. Customer will also be responsible for all Electronic Communications, including those containing business information, account registration, account holder information, financial information, Customer Data, and all other data of any kind contained within emails or otherwise entered electronically through the RFgen Service or under Customer's account. RFgen will act as though any Electronic Communications it receives under Customer's passwords, user name, and/or account number will have been sent by Customer. Customer shall use commercially reasonable efforts to prevent unauthorized access to or use of the RFgen Service and shall promptly notify RFgen of any unauthorized access or use of the RFgen Service and any loss or theft or unauthorized use of any User's password or name associated with the RFgen Service.

6. TRANSMISSION OF DATA.

Customer understands that the technical processing and transmission of Customer's Electronic Communications is fundamentally necessary to use of the RFgen Service. Customer is responsible for securing DSL, cable or another high-speed Internet connection in order to utilize the RFgen Service. Customer expressly consents to RFgen's interception and storage of Electronic Communications and/or Customer Data as needed to provide the Services hereunder, and Customer acknowledges and understands that Customer's Electronic Communications will involve transmission over the Internet, and over various networks, only part of which may be owned and/or operated by RFgen. Customer further acknowledges and understands that Electronic Communications may be accessed by unauthorized parties when communicated across the Internet, network communications facilities, telephone or other electronic means. Without limiting RFgen's applicable obligations under the Security or Confidentiality Sections of the Services Agreement, RFgen is not responsible for any Electronic Communications and/or Customer Data which are delayed, lost, altered, intercepted, or stored during the transmission of any data whatsoever across networks not owned and/or operated by RFgen, including, but not limited to, the Internet and Customer's local network.

7. THIRD-PARTY APPLICATIONS.

RFgen or third-party providers may offer Third Party Applications. Except as expressly set forth in the Order, RFgen does not warrant any such Third-Party Applications, regardless of whether or not such Third-Party Applications are provided by a third party that is a member of an RFgen partner program or otherwise designated by RFgen as "**certified**", "**approved**", or "**recommended**". Any procurement by Customer of such Third-Party Applications or services is solely between Customer and the applicable third-party provider.

RFgen is not responsible for any aspect of such Third-Party Applications that Customer may procure or connect to through the RFgen Service, or any interoperation, descriptions, promises, or other information related to the foregoing. If Customer installs or enables Third Party Applications for use with the RFgen Service, Customer agrees that RFgen may enable such third party providers to access Customer Data for the interoperation of such Third Party Applications with the RFgen Service, and any exchange of data or other interaction between Customer and a third party provider is solely between Customer and such third party provider pursuant to a separate privacy policy or other terms governing Customer's access to or use of the Third Party Applications. RFgen shall not be responsible for any disclosure, modification or deletion of Customer Data resulting from any such access by Third Party Applications or third-party providers. No procurement of such Third-Party Applications is required to use the RFgen Service. If Customer was referred to RFgen by a member of one of RFgen's partner programs, Customer hereby authorizes RFgen, or its applicable affiliate, to provide such member or its successor entity with access to Customer's business information related to the procurement and use of the RFgen Service pursuant to this Agreement, including but not limited to server and license count, implemented workflows, support cases, and billing/payment information.

8. SERVICE MONITORING AND ANALYSES.

RFgen continuously monitors the RFgen Service to facilitate RFgen's operation of the Services; to help resolve Customer service requests; to detect and address threats to the functionality, security, integrity, and availability of the Services as well as any content, data, or applications in the Services; and to detect and address illegal acts or violations of the Acceptable Use Policy. RFgen monitoring tools do not collect or store any Customer Data residing in the Services, except as needed for such purposes. RFgen does not monitor, and does not address issues with, non-RFgen software provided by Customer or any of Customer's Users that is stored in, or run on or through, the Services. Information collected by RFgen monitoring tools (excluding Customer Data) may also be used to assist in managing RFgen's product and service portfolio, to help RFgen address deficiencies in its product and service offerings, and for license management purposes.

RFgen may (i) compile statistical and other information related to the performance, operation, and use of the Services, and (ii) use data from the Services in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (clauses (i) and (ii) are collectively referred to as "**Service Analyses**"). RFgen may make Service Analyses publicly available; however, Service Analyses will not incorporate Customer Data, personal information or Confidential Information in a form that could serve to identify Customer or any individual. RFgen retains all intellectual property rights in Service Analyses.

9. PCI-DSS COMPLIANCE.

Customer is responsible for ensuring that its use of the RFgen Service to store or process credit card data complies with applicable Payment Card Industry Data Security Standards ("**PCI DSS**") requirements and shall not store credit card and

social security data in the RFgen Service except in the designated encrypted fields for such data. During the Term, RFgen shall maintain PCI DSS compliance for those portions of the RFgen Service that are designated by RFgen as being designed to store and process credit card data. Any changes made to the RFgen Service by the Customer or at the Customer's direction may affect the Customer's compliance with PCI DSS requirements and Customer shall be solely responsible for ensuring that any such changes are compliant with PCI DSS requirements.