RFgen Corporate Security Policy

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**"), a global provider of enterprise mobility solutions, delivers leading edge capabilities in extending manufacturing, warehousing, and maintenance operations onto mobile devices, supporting businesses both in the cloud and on premise.
RFgen's security practices are multidimensional and reflect the various ways RFgen engages with its customers:

RFgen's Corporate Security Practices ("**Security Practices**") are implemented pursuant to RFgen's Corporate security programs and guide RFgen for its operational and services infrastructure under its control, including RFgen's corporate network and systems.

- The term "**customer data**" as used in this document means any data stored in a customer's computer system (data accessed by or provided to RFgen while performing services for a customer) or customer's RFgen cloud instance.
- Third parties who have been provided access to customer data by RFgen ("**sub-processors**") are required to contractually commit to materially equivalent security practices.

RFgen continually works to strengthen and improve the security controls and practices for RFgen internal operations and services offered to customers. These practices are subject to change at RFgen's discretion. Companies that RFgen acquires are required to align with these Security Practices as part of the integration process.

The purpose of this paper is to summarize key RFgen's security practices and programs. This paper does not exhaustively describe other security practices and programs which may be applicable and relevant to individual lines of business or services that may be procured by a customer.

1. RFGEN INFORMATION SECURITY

RFgen's Corporate Security Programs are designed to protect both RFgen and customer data, such as:

- The mission-critical systems that customers rely upon for cloud services, technical support and other services.
- RFgen source code and other sensitive data against theft and malicious alteration.
- Personal and other sensitive information that RFgen collects in the course of its business, including customer, partner, supplier and employee data residing in RFgen's internal IT systems.

RFgen's security policies cover the management of security for both RFgen's internal operations and the services RFgen provides to its customers, and apply to all RFgen personnel, such as employees and contractors. These policies are generally aligned with the ISO/IEC 27002:2022 and ISO/IEC 27001:2013 standards and guide all areas of security within RFgen.

Reflecting the recommended practices in security standards issued by the International Organization for Standardization (ISO), the United States National Institute of Standards and Technology (NIST), and other industry sources, RFgen has implemented a wide variety of preventive, detective, and corrective security controls with the objective of protecting information assets.

2. ORGANIZATIONAL SECURITY

The Chief Information Officer is one of the directors of the RFgen Security Oversight Committee (RSOC). The Chief Information Officer manages the Corporate Security department which guides security at RFgen. This department drives corporate security programs, defines corporate security policies, and provides global oversight for RFgen's security policies and requirements.

RFgen Security Oversight Committee

The RFgen Security Oversight Committee (RSOC) oversees the implementation of RFgen-wide security programs, including security policies and data privacy standards. The RSOC is chaired by RFgen's CEO, General Counsel, Chief Information Officer, and Technical Communications Program Manager. RSOC oversees the following areas of corporate governance.

Information Security. Global Information Security policies cover the management of information security across RFgen including:

- Advice to help protect RFgen information assets (data), as well as the data entrusted to RFgen by our customers, partners, and employees.
- Coordination of reporting of information security risk to senior leadership such as the RFgen Security Oversight Committee and Board of Directors.
- Direct and advise on the protection of data developed, accessed, used, maintained, and hosted by RFgen.
- IT security strategy, architectural design of security solutions, engineering, risk management, security infrastructure operations and support, standards and compliance, threat intelligence and remediation, and security technical assessment for new infrastructure.

Product Security. Covers policies designed to help RFgen development teams improve the security of RFgen products. Encompassing every phase of the product development lifecycle, product security defines RFgen's methodology for building security into the design, build, test, and maintenance of its products.

Physical Security. Covers policies for defining, developing, implementing, and managing all aspects of physical security for the protection of RFgen's employees, facilities, business enterprise, and assets.

3. PRIVACY.

The RFgen General Privacy Policy addresses information we collect in connection with your use of RFgen websites, mobile applications, and social media pages that link to the General Privacy Policy, your interactions with RFgen during in-person meetings at RFgen facilities or at RFgen events, and in the context of other online or offline sales and marketing activities.

The Services Privacy Policy describes our privacy and security practices that apply when handling (i) services personal information in order to perform Consulting, Technical Support, Cloud and other services on behalf of RFgen customers.

4. CUSTOMER DATA PROTECTION.

RFgen's media sanitation and disposal policy defines requirements for removal of information from electronic storage media (sanitization) and disposal of information which is no longer required to protect against unauthorized retrieval and reconstruction of confidential data. Electronic storage media includes laptops, hard drives, storage devices and removable media such as tape.

5. ASSET CLASSIFICATION AND CONTROL.

Developing and maintaining accurate system inventory is a necessary element for effective general information systems management and operational security. RFgen's information systems asset inventory policy requires that all business units maintain accurate and comprehensive inventories of information systems, hardware, and software. This policy applies to all information assets held on any RFgen system, including both enterprise systems and cloud services.

RFgen categorizes information into three classes —Public, Internal, and Restricted— with each classification requiring corresponding levels of security controls, such as encryption requirements for non-Public data:

- "**Public**" information is intended for public consumption and can be shared without any negative implications.
- "**Internal**" or Internal Use Only information is available to employees and authorized non-employees (consultants and contractors) possessing a **need to know for business related purposes**.
- "**Confidential**" information that is intended for use only by specified groups of employees. A breach of such information could cause serious embarrassment and possibly undermine public trust in the organization. It must remain confidential to RFgen and access within RFgen must be restricted on a "**need to know**" basis.
- "**Sensitive**" information is protected by international, federal, state, or local laws or regulations, or industry standards. Examples of state data protection laws include HIPAA/HITECH, the GDPR, PCI-DSS, and Executive

Order 13556 (related to controlled unclassified information (CUI). A breach of such information could cause government fines as well as undermine public trust in the organization.

RFgen has formal requirements for accessing, handling, and retaining of each class of data; These operational policies (i.e. Data Classification policy) define requirements per data type and category, including examples of records in various RFgen departments. Retention of customer data in cloud services is controlled by the customer and is subject to terms in their contract.

Customer data is classified as Internal or Confidential for the purpose of placing limits on access, distribution, and handling of such data. RFgen keeps the information confidential in accordance with the terms of customer's order.

6. HUMAN RESOURCES SECURITY.

RFgen places a strong emphasis on personnel security. The company maintains ongoing initiatives intended to help minimize risks associated with human error, theft, fraud, and misuse of facilities, including personnel screening, confidentiality agreements, security awareness education and training, and enforcement of disciplinary actions.

RFgen maintains high standards for ethical business conduct at every level of the organization, and at every location where RFgen does business around the world. These apply to RFgen employees, contractors, and temporary employees, and cover legal and regulatory compliance and business conduct and relationships. RFgen requires its employees to receive training in ethics and business conduct every two years.

Employees who fail to comply with RFgen policies, procedures and guidelines may be subject to disciplinary action up to and including termination of employment.

7. PHYSICAL SECURITY.

Physical Security policies are responsible for defining, developing, implementing, and managing all aspects of physical security for the protection of RFgen's employees, facilities, business enterprise, and assets. RFgen regularly performs risk assessments to confirm that appropriate mitigation controls are in place and maintained.

RFgen currently has implemented the following protocols:

- Physical access to facilities is limited to RFgen employees, contractors, and authorized visitors.
- Visitors are required to sign a visitor's register, be escorted and/or observed when they are on RFgen premises, and/or be bound by the terms of a confidentiality agreement with RFgen.
- Security monitors the possession of keys/access cards and the ability to access facilities. Staff leaving RFgen's employment must return keys/cards and key/cards are deactivated upon termination.
- Security authorizes all repairs and modifications to the physical security barriers or entry controls at service locations.
- RFgen has implemented centrally managed electronic access control systems with integrated intruder alarm capability.

8. OPERATIONS MANAGEMENT.

Protection Against Malicious Code. RFgen policy requires the use of antivirus protection and firewall software on endpoint devices such as laptops, desktops, and mobile devices. Additionally, all computers running a Windows operating system that hold RFgen data must have automated Microsoft security updates enabled. Security updates for all other devices and operating systems must be installed upon notification of their availability. Desktops and laptops that process RFgen or customer information must be encrypted using approved software.

Antivirus software must be scheduled to perform daily threat-definition updates and virus scans.

The RFgen's Information Technology group keeps antivirus products and Windows Server Update Services (WSUS) up to date with virus definitions and security updates and is responsible for notifying internal RFgen system users of both any credible virus threats and when security updates are available.

Employees are prohibited from altering, disabling, or removing antivirus software and the security update service from any computer. Any RFgen employee who is discovered violating this standard may be subject to disciplinary action up to and including termination of employment.

Monitoring and Protection of Audit Log Information. RFgen logs certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to RFgen programs, as well as system alerts, console messages and system errors. RFgen implements controls designed to protect against operational problems, including log file media becoming exhausted, failing to record events and/or logs being overwritten.

RFgen periodically reviews logs for forensic purposes and incidents. Identified anomalous activities feed into the security-incident management process. Access to security logs is provided on a need-to-know and least privilege. Where available for cloud services, log files are protected by strong cryptography in addition to other security controls, and access is monitored. Logs generated by internet-accessible systems are relocated to systems that are not internet-accessible.

Network Controls. RFgen has implemented and maintains strong network controls for the protection and control of both RFgen and customer data during its transmission. RFgen's network security policy establishes requirements for network management, network access and network device management, including authentication and authorization requirements for both physical devices and software-based systems. Unused network ports must be deactivated.

For administration of network security and network-management devices, RFgen requires IT personnel to use secure protocols with authentication, authorization, and strong encryption. Network devices must be located in an environment protected with physical access controls as defined by Physical Security policies.

Communications to and from the RFgen corporate network must pass through network security devices at the border of RFgen's internal corporate network. Remote connections to the RFgen corporate network must exclusively use approved virtual private networks (VPNs). Corporate systems available outside the corporate network are protected by alternative security controls such as multifactor authentication.

RFgen's network security policy establishes formal requirements for the provision and use of wireless networks and connectivity to access the RFgen corporate network, including network segmentation requirements. RFgen's IT group manages wireless networks and monitors for unauthorized wireless networks.

9. ACCESS CONTROL.

Access control refers to the policies, procedures and tools that govern access to and use of resources. Examples of resources include a physical server, file, application, data in a database and network device.

- Least privilege is a system-oriented approach in which user permissions and system functionality are carefully evaluated and access is restricted to the resources required for users or systems to perform their duties.
- Default-deny is a network-oriented configuration approach that implicitly denies the transmission of all traffic, and then specifically allows only required traffic based on protocol, port, source network address, and destination network address.

RFgen's logical access control policy is applicable to access control decisions for all RFgen employees and any information-processing facility for which RFgen has administrative authority. Logical access controls for applications and systems must provide identification, authentication, authorization, accountability, and auditing functionality. This policy does not apply to customer end user accounts for RFgen services customers.

User Access Management. Access privileges are granted based on job roles and require management approval. Operations are organized into functional groups, where each function is performed by separate groups of employees. Examples of functional groups include developers, implementation consultants, system administrators, and support technicians.

Privilege Management. Authorization is dependent on successful authentication, since controlling access to specific resources depends upon establishing an entity or individual's identity. All RFgen authorization decisions for granting, approval and review of access are based on the following principles:

- Need to know: Does the user require this access for their job function?

- Segregation of duties: Will the access result in a conflict of interest?
- Least privilege: Is access restricted to only those resources and information required for a legitimate business purpose?

Password Management. RFgen has strong password policies (including length and complexity requirements) for the RFgen network, operating system, email, database, and other accounts to reduce the chances of intruders gaining access to systems or environments through exploitation of user accounts and associated passwords. System-generated and assigned passwords are required to be changed immediately on receipt.

RFgen personnel are obligated to follow rules for password length complexity, as well as other password requirements. Employees must keep their passwords confidential and secure and are prohibited from sharing their individual account passwords with anyone, whether verbally, in writing, or by any other means. Employees are not permitted to use any RFgen system or applications passwords for non-RFgen applications or systems.

Periodic Review of Access Rights. RFgen regularly reviews network and operating system accounts with regard to the appropriate employee access levels. In the event of employee terminations, deaths, or resignations, RFgen takes appropriate actions to promptly terminate network, email, telephony, and physical access.

10. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT, AND MAINTENANCE.

RFgen policy requires that appropriate security maintenance be performed against RFgen's information systems. This includes the deployment of security patches in RFgen technology as well as associated recommendations. Additionally, this policy includes requirements for applying relevant security updates for any non-RFgen technology in RFgen's information systems.

The section "**RFgen Security Assurance**" later in this paper describes development practices to minimize the risk of introduction of security defects (i.e., security bugs) in RFgen code.

The RFgen Server Security Policy requires servers (both physical and virtual) managed by RFgen or third parties on behalf of RFgen to be physically and logically secured to prevent unauthorized access to the servers and associated information assets.

11. INFORMATION SECURITY INCIDENT RESPONSE.

Reflecting the recommended practices in prevalent security standards issued by the International Organization for Standardization (ISO), the United States National Institute of Standards and Technology (NIST), and other industry sources, RFgen has implemented a wide variety of preventive, detective, and corrective security controls with the objective of protecting information assets.

RFgen will evaluate and respond to any event when RFgen suspects that RFgen-managed customer data has been improperly handled or accessed. RFgen's Information Security Incident Reporting and Response Policy defines requirements for reporting and responding to events and incidents. This policy authorizes the RFgen Security Oversight Committee (RSOC) to provide overall direction for incident prevention, identification, investigation, and resolution within RFgen's individual business units.

Upon discovery of an incident, RFgen defines an incident-response plan for rapid and effective incident investigation, response, and recovery. Root-cause analysis is performed to identify opportunities for reasonable measures which improve security posture and defense in depth. Formal procedures and systems are utilized to collect information and maintain a chain of custody for evidence during incident investigation.

If RFgen determines that a confirmed security incident involving Personal Information processed by RFgen has taken place, RFgen will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the RFgen Subscription and Services Agreement. Information about malicious attempts or suspected incidents is treated as RFgen Confidential information and is not externally shared. Incident history is also considered as RFgen Confidential information and is not shared externally.

12. RFGEN SECURITY ASSURANCE (RSA).

Encompassing every phase of the product development lifecycle, RFgen Security Assurance (RSA) is RFgen's methodology for building security into the design, build, testing and maintenance of its products, whether they are used on-premises by customers or delivered through RFgen cloud services.

RFgen's goal is to ensure that RFgen's products help customers meet their security requirements while providing the most cost-effective ownership experience.

RFgen Security Assurance is a set of industry-leading standards, technologies, and practices aimed at:

- Fostering security innovations. RFgen has a long tradition of security innovations. Today this legacy continues with solutions that help organizations implement and manage consistent security controls across the technical environments in which they operate, on-premises and in the clouds.
- Reducing the incidence of security weaknesses in all RFgen products. RFgen Security Assurance key programs include RFgen's Secure Coding Standards, mandatory security training for development, the cultivation of security leaders within development groups, and the use of automated analysis and testing tools.
- Reducing the impact of security weaknesses in released products on customers. RFgen has adopted transparent security vulnerability disclosure and remediation policies. The company is committed to treating all customers equally and delivering the best possible security patching experience through the Critical Patch Update and Security Alert programs.

Coding Standards & Security Training. Developing secure software requires consistently applied methodologies across the organization that conform to stated policies, objectives, and principles. RFgen's objective is to produce secure code. To that end, RFgen requires that all development abide by secure coding principles that have been documented and maintained to remain relevant. Additionally, RFgen has adapted its secure coding principles for use by our consulting and services organizations when they are engaged in producing code on behalf of our customers.

RFgen Secure Coding Standards are a roadmap and guide for developers in their efforts to produce secure code. They discuss general security knowledge areas such as design principles, cryptography and communications security, common vulnerabilities, etc., and provide specific guidance on topics such as data validation and user management.

All RFgen developers must be familiar with these standards and apply them when designing and building products. The coding standards have been developed over several years and incorporate best practices as well as lessons learned from continued vulnerability testing by RFgen's internal product assessment team. RFgen ensures that developers are familiar with its coding standards by requiring that they undergo secure coding training. The Secure Coding Standards are a key component of RFgen Security Assurance and adherence to the Standards is assessed and validated throughout the supported life of all RFgen products.

Security Analysis & Testing. Security testing of RFgen code includes both functional and non-functional activities for verification of product features and quality. Although these types of tests often target overlapping product features, they have orthogonal goals and are carried out by different teams. Functional and non-functional security tests complement each other to provide comprehensive security coverage of RFgen products.

Functional security testing is typically executed by regular product Quality Assurance (QA) teams as part of the normal product testing cycle. During this testing, QA engineers verify conformance of implemented security features to what had been previously agreed upon in the functional specifications during the architectural and checklist reviews process.

Security assurance analysis and testing verify security qualities of RFgen products against various types of attacks. There are two broad categories of tests employed for testing RFgen products: static and dynamic analysis:

- Static security analysis of source code is the initial line of defense used during the product development cycle using up-to-date, commercially available tools, to help catch problems while code is being written.
- Dynamic analysis activity takes place during latter phases of product development. Dynamic analysis is aimed at externally visible product interfaces and APIs, and frequently relies on specialized tools for testing. Both manual and automatic tools are used for testing within RFgen. Automatic tools generally test network-accessible product interfaces and protocols, while manual tools validate scripting accessible API's.

Critical Patch Updates. The Critical Patch Update (CPU) is the primary mechanism for the provision of security bug fixes and changes necessary for continued integration into supported ERP systems for all RFgen product distributions. Critical Patch Updates are available to customers with valid support contracts and/or active subscription agreements. Critical Patch Updates are released whenever critical vulnerabilities and/or when active exploits are reported in the wild or notification has been received that an ERP API in use has been marked for deprecation. This program is known as the Security Alert program. Customers are notified whenever a CPU is available for their environment and can schedule an appropriate time for installation.

Vulnerabilities identified are remediated by RFgen in order of the risk they pose to users. This process is designed to patch the security defects with the greatest associated risk first in the Critical Patch Update, resulting in optimizing the security posture of all RFgen customers.

Patch updates are cumulative for many RFgen products. This provides customers the ability to catch up quickly to the current security release level, since the application of the latest cumulative CPU resolves all previously addressed vulnerabilities.

Source Code Protection. RFgen maintains strong security controls over its source code. RFgen's source-code protection policies provide limits on access to source code (enforcement of the need to know), requirements for independent code review, and periodic auditing of the company's source-code repositories.

RFgen Security Assurance policies and practices are designed to prevent the introduction of security vulnerabilities in RFgen-developed code. Additionally, RFgen maintains strong controls over the technical description of security vulnerabilities in RFgen code. RFgen's Security Vulnerability Information Protection Policy defines the classification and handling of information related to product security vulnerabilities and requires that information concerning security bugs be recorded in a tightly controlled database.

Note that RFgen's policies prohibit the introduction of backdoors into its products. Backdoors are deliberately (and maliciously) introduced code intended to bypass the security controls of the application in which it is embedded. Backdoors do not include:

- Unintentional defects in software that could lead to a weakening of security controls (security bugs.)
- Undocumented functionality designed to be generally inaccessible by customers but serves a valid business or technical purpose (diagnostics and troubleshooting utilities.)

RFgen assesses third-party software and hardware to avoid the use of products:

- With known vulnerabilities.
- Developed with poor security assurance.
- That may potentially include backdoors.

External ERP Evaluations. RFgen submits certain products for external connectivity and integration evaluations / validations. These evaluations involve rigorous testing by specialist ERP staff (SAP, Oracle, etc.) with further oversight and certification meeting their published standards. Independent verification helps provide additional assurance to RFgen customers with regards to the integration and security posture of the validated products. Additionally, customers in many industries have business and compliance requirements that imply the use of validated products.

13. RESILIENCE MANAGEMENT.

RFgen's risk management resiliency policy defines requirements and standards for all RFgen business unit plans for response to business disruption events. It also specifies the functional roles and responsibilities required to create, maintain, test, and evaluate business continuity capability for RFgen across lines of business and geographies. It defines the compliance oversight responsibilities for the program. The policy mandates an annual operational review for planning, evaluation, training, validation, and executive approvals for critical business operations.

The program's key objective is to establish a business-resiliency framework to help provide an efficient response to business interruption events affecting RFgen's operations. Its approach is comprised of several subprograms: emergency response to unplanned and emergent events, crisis management of serious incidents, technology disaster recovery, and

business-continuity management. The goal of the program is to minimize negative impacts to RFgen and its customers while maintaining critical business processes until regular operating conditions are restored.