GENROCKET SECURITY CHECKLIST

GENROCKET CLOUD			
	FEATURES	SECURITY PROVISIONS	THREAT PROTECTION
1	**Architecture**	The GenRocket solution is implemented in a *secure hybrid cloud computing environment* that separates the process of configuring synthetic test data from generating synthetic test data.	Test data design takes place in the cloud, while test data generation takes place on-premises and behind the customer's corporate firewall.
2	**Synthetic Test Data**	Synthetic data is not real data and is not sourced from a production database, so it's 100% secure. There is no requirement for masking or anonymizing sensitive data because no personal or private data is used in the generation of synthetic data.	Synthetic data is artificial data matching the data structure of the target data environment. This results in test data that fully meets the requirements of all data privacy laws such as GLBA, HIPAA, and GDPR
3	**Customer Data**	At no time is any confidential data that is subject to regulatory compliance frameworks contained in *GenRocket Cloud* or on customer premises in *GenRocket Runtime*.	There is no possibility of access to, or exposure of, customer data of any kind, at any time.
4	**Meta Data**	GenRocket imports metadata (e.g., database schema) to generate an accurate representation of the target data environment. This is done on-prem behind the corporate firewall, then transferred to *GenRocket Cloud* via secure encrypted tunnel. Once synthetic data has been modeled, the original meta data file is purged from the system.	No metadata is ever at risk of exposure because it is always behind a firewall or transported over secure encrypted sessions. Only authorized and authenticated users may handle metadata files.

	FEATURES	SECURITY PROVISIONS	THREAT PROTECTION
5	**Configuration Files**	Through the self service components in *GenRocket Cloud,* users design the synthetic data needed for testing. *Test Data Design Files* provide the instructions needed for generating data in real-time and on-demand.	*Test Data Design* Files contain no customer data. They are small XML files that tell the *GenRocket Runtime* how to use data generators and receivers to produce the volume and variation of data needed for testing.
6	**Hosting Environment**	*GenRocket Cloud* is hosted by AWS, one of the most advanced hosting environments in the world in terms of security, availability, and scalability. AWS is fully certified as an *ISO 27001* compliant computing environment	Through AWS, GenRocket provides its customers with the highest possible level of application and network security for conducting *Test Data Automation* operations.
7	**Infrastructure**	The GenRocket application and its system resources are contained in a Virtual Private Cloud (VPC) to provide a secure multitenant environment. A public subnet connects an AWS Internet Gateway to the Internet and a private subnet, inaccessible by Internet connected systems, houses the system resources that operate customer instances of *GenRocket Cloud*.	Resources on the VPC are not accessible by the public Internet other than by connecting through Network Address Translation (NAT) contained in a secure Internet Gateway. Access to the VCP requires users to be authenticated and authorized to use the system.
8	**Deployment Options**	While the vast majority of GenRocket customers are hosted in a secure VPC environment, a Dedicated Private Cloud (DPC) is optionally available. A DPC provides the same resources contained in the VPC infrastructure except they are dedicated to a single customer and partitioned from other accounts. DPC hosting is available on request for an additional charge.	GenRocket software has been continuously updated over the last 8 years to address emerging security threats and vulnerabilities. GenRocket is committed to providing the highest level of security and will deploy the GenRocket Cloud application to a shared or dedicated private cloud as the customer deems appropriate. Dedicated on-premise hosting is also available if the customer requires it for an additional free.
9	**Access Management**	Access to *GenRocket Cloud* is restricted to authorized and authenticated users who are licensed to operate GenRocket software. Users can only be added by an organization admin and they are assigned user privileges to access only the specific information or resources appropriate for their role.	*GenRocket Cloud* security provisions eliminate the possibility of unauthorized access from either inside or outside of the customers organization

GENROCKET RUNTIME			
	FEATURES	SECURITY PROVISIONS	THREAT PROTECTION
10	**On-Prem Deployment**	*The GenRocket Runtime* is a collection of secure Java JARs (Java Archive Files) that act as the engine for synthetic test data generation. It is located on-premise, and behind the secure protection of the corporate firewall.	*The GenRocket Runtime* is not a standalone application that represents a new security threat to the local environment. It leverages the Java Runtime Environment (version 1.7 or later) to perform data generation related tasks.
11	**Java Runtime**	GenRocket JARs contained compiled code that is purpose-built for the GenRocket platform. All JARs are validated with a checksum to ensure they have not been tampered with in any way. If they have been altered, they will fail the checksum validation process and will not operate.	There is no risk of malicious code entering the system through the alteration of GenRocket JARs that comprise GenRocket Runtime.
12	**Instruction Sets (Scenarios) and Configuration Files (Test Data Cases)**	*The GenRocket Runtime* uses *Test Data Design Files* created in the *GenRocket Cloud* to generate synthetic data. The Test Data Design Files themselves contain no data and can only be accessed by licensed, authenticated and authorized users.	No production data is used in the generation of synthetic test data. No data generation takes place outside of the secure corporate environment. Only approved users have access to *Test Data Design* Files and they only have access to resources specific to their projects as defined by their access rights.
13	**Test Data Generation**	All data generated by GenRocket is 100% synthetic data based on pre-defined *Test Data Design Files*, not by copying, anonymizing, or virtualizing a production database. A synthetic test dataset is 100% safe and secure.	There is no possibility of sensitive customer data being accessed, copied, exported or exposed in any way.
14	**G-Repository**	All *Test Data Design Files* are stored in an on-premise repository called *G-Repository* Server which synchronizes with *G-Repository* Clients on each test automation server or tester's machine located wthin a secure on-premise environment.	*G-Repository automates the management and maintenance of Test Data Design Files.* It automatically synchronizes changes and ensures strict revision control over project work. *G-Repository* Server always communicates with its related system component, G-Repository Client, inside a secure corporate environment.

SECURE CONNECTIVITY			
	FEATURES	SECURITY PROVISIONS	THREAT PROTECTION
15	**User Authentication**	Users access *GenRocket Cloud* using Chrome, Firefox, or Safari browsers using HTTPS with *Transport Layer Security* (TLS) version 1.2 to authenticate and encrypt their sessions. Users provide a valid user name and password that must adhere to the customer's password complexity requirements.	GenRocket uses the TLS standard to ensure the highest level of security between the user and their *GenRocket Cloud* account. This prevents unauthorized access to resources and/or eavesdropping of session information conveyed over the Internet.
16	**Single Sign on**	For an additional layer of security, GenRocket customers can elect to use a centralized identity management service (e.g., Active Directory) to perform user authentication.	SSO allows centralized control over the identity management process by a directory server maintained by the customer's security team.
17	**User Authorization**	The *GenRocket Team Permissions* feature ensures users are only able to access the appropriate projects for their role and manages permitted information within those projects.	*Team Permissions* prevents unauthorized access to test data projects and unwanted changes to Scenarios and test Data Cases stored in G-Repository.
18	**User Profile**	A *User Profile* is an encrypted file that contains information for a user to operate *GenRocket Runtime*. It also contains information allowing the user to connect to non-GenRocket systems and databases. This information is created and stored in the user's local machine and known only to the user.	GenRocket does not have access to any system login credentials within the customer's corporate environment that are associated with a User Profile
19	**Session Encryption**	All connections between a user and *GenRocket Cloud* or between *GenRocket Cloud* and *GenRocket Runtime* are encrypted by TLS 1.2 encryption.	The connections from *GenRocket Cloud* to *GenRocket Runtime* or from *GenRocket Cloud* to Internet-connected users are encrypted to prevent unauthorized access or exposure of session information.
20	**Checksum Validation**	GenRocket performs a checksum validation of all transited files between GenRocket Cloud and GenRocket Runtime to prevent tampering with their contents by non-GenRocket individuals.	Any file that fails checksum validation will not be used by the system. This prevents the injection of malware or malicious code at all times.

ADMINISTRATION			
	FEATURES	SECURITY PROVISIONS	THREAT PROTECTION
21	**Security Assessments**	External 3rd party penetration testing conducted by a recognized expert security firm is conducted annually. Internal penetration testing is conducted every 90 days. GenRocket has also commissioned an assessment of its platform to be performed and documented by an authoritative information and technology security analyst (available on our website).	GenRocket is committed to maintaining the highest level of security to preserve its nine-year track record of delivering its *Synthetic Test Data Automation* solution free of security incidents.
22	**Disaster Recovery**	The GenRocket primary AWS data center is in Virginia and a backup facility has been established 2,500 miles away in Oregon. Each location houses an AWS Region consisting of multiple, isolated, physically separate Availability Zones (AZ). Each AZ has independent cooling, power, and physical security.	*GenRocket Cloud* represent a high availability operating environment with sophisticated disaster recovery provisions that ensure continuous operations with minimal system downtime.
23	**Data Backup**	An hourly database dump is taken to secondary *Region* (Oregon), So in case of data loss on the production *Region* (Virginia) data can be replicated on the backup facility.	A fresh data backup is always available to restore any information lost due to a potential system failure or security incident.
24	**System Administration**	All users are assigned licenses and system privileges by an organization administrator. The Org Admin is a trusted user appointed by the customer with full access to GenRocket system resources.	Non-licensed users may not access the GenRocket platform and licensed users can only access resources based on their permission level.