ROSALIND

Organizational & Hosting Platform Security Measures

Updated August 2018

1. **Security Management.** Security Management is overseen by Chief Product Officer and is reviewed on a regular basis with the CEO.

2. **ROSALIND Hosting Partner.** ROSALIND is hosted on Google Cloud Platform with potential region specific instances and data storage. Typically, ROSALIND operates from the Google Data Centers in Iowa and South Carolina, unless otherwise specified and agreed.

3. **Data at Rest Encryption.** ROSALIND leverages the world-class encryption as provided by Google Cloud Platform without need for further configuration. Data is automatically encrypted prior to being written to disk. Each encryption key is itself encrypted with a set of master keys. Keys and encryption policies are managed the same way, in the same keystore, as for Google's production services.

4. **Data in Motion Encryption.** ROSALIND encryption also includes encryption for data in motion, as provided by Google Cloud. Additionally, ROSALIND Bio uses SSL and certificates to secure all communications between clients and the ROSALIND SaaS solution. ROSALIND uses ports 443 (SSL), 80 (HTTP) and 8080 (API) for data communication between clients and ROSALIND.

5. **Change Control Processes.** ROSALIND maintains formal development and bug management processes, including changes to ROSALIND core operating code and systems, as well as Google Cloud Platform infrastructure. 4 distinct environments and levels of development and testing are used to validate and control changes to ROSALIND, including dev, stage, beta and live.

6. **Hosting Provider - Independent Certifications.** Google Cloud Platform is certified for NIST 800-53, NIST 800-171, COBIT-5. Google Cloud Platform conducts rigorous internal continuous testing of our application surface through various types of penetration exercises. In addition, Google Cloud Platform coordinates external 3rd party penetration testing using qualified and certified penetration testers.

7. **Hosting Provider - Independent Audit Reports.** Google Cloud Platform undergoes several independent third party audits to test for data safety, privacy, and security, as noted below: SOC 1 / 2 / 3 (Formerly SSAE16 or SAS 70) ISO 27001 ISO 27017 / 27018 PCI-DSS HIPAA. Google Cloud Platform Security Policy prohibits sharing this information but customers may conduct their own testing on our products and services. Google Cloud Platform publishes and makes available its ISO 27001, 27017, 27018 and SOC3 reports online.

8. **Hosting Provider - Secure Areas.** Google Cloud Platform maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are

allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and requires the approval of the requestor’s manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations (iii) and reference an approved data center access record identifying the individual as approved.

9. **Hosting Provider - Physical Areas.** Google Cloud Platform maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and requires the approval of the requestor’s manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations (iii) and reference an approved data center access record identifying the individual as approved.