Data and Security Policy

Updated July 2018

1. Environment

ROSALIND shall securely process, host, transmit, and store the Customer Data. ROSALIND shall provide the Service using no less than generally accepted industry practice physical and environmental security measures designed to prevent unauthorized access to, theft of, or unlawful disclosure of the Customer Data. ROSALIND shall employ technologies that are consistent with industry standards for firewalls and other security technologies. ROSALIND shall notify Customer of each location for storing data.

2. Data Transfers

ROSALIND shall use Secure Sockets Layer ("SSL") standards, or then-current successor protocols, designed to protect data confidentiality during transfers. In addition, ROSALIND shall maintain at a minimum the following security measures: HTTP with SSL 256-bit encryption ("HTTPS"); at least 256-bit AES encryption and encode data during transmission; and encrypted passwords for hosting services.

3. Information Security Program

ROSALIND shall establish, implement, and maintain an information security program that includes technical and organizational security and physical measures as well as policies and procedures designed to protect Customer Data processed by ROSALIND against accidental loss; destruction or alteration; unauthorized disclosure or access; or unlawful destruction. OnRamp's information security program must reasonably address the confidentiality, integrity, and availability of all Customer Data, including the below matters and any other requirements specified in this attachment:

a) Periodic risk assessments.
b) Identification and documentation of the security requirements of authorized users.
c) User access, the nature of that access, and authorization of access.
d) Prevention of unauthorized access through the use of effective physical and logical access controls.
e) Procedures to manage system-level access.
f) Assignment of responsibility and accountability for security and for system changes and maintenance.
g) Implementation of system software upgrades and patches, including a patching review interval of once per calendar quarter for security impacting patches. In addition to this regular patching review schedule, ROSALIND shall implement appropriate patches if it becomes aware at any time of a security vulnerability and ROSALIND shall implement critical patches as soon as possible.
h) Testing, evaluating, and authorizing system components before implementation.
i) Resolution of complaints and requests relating to security issues.
j) Handling of errors and omissions, security breaches, and other incidents.
k) Procedures to detect actual and attempted attacks or intrusions into systems and to proactively test security procedures (for example, penetration testing).
l) Allocation of training and other resources to support its security policies.
m) Risk and security incident management.
n) Processing integrity and related system security policies.

o) A requirement that users, management, and third parties confirm (initially and annually) their understanding of an agreement to comply with the applicable privacy policies and procedures related to the security of Customer Data.
p) Procedures for proper destruction and disposal of Customer Data.

4. Audit and Test

Customer may conduct non-intrusive network audits (basic port scans, etc.) with reasonable prior notice. Customer shall not attempt to access the data of another ROSALIND customer. Customer may perform any technical security integrity review, penetration test, load test, denial-of-service simulation or vulnerability scan with ROSALIND's prior written consent.

5. Mitigation of Vulnerabilities

ROSALIND shall promptly mitigate any critical security vulnerabilities discovered at any time.

6. Notification of Security Breach

Upon becoming aware of any unlawful or unauthorized access to any Customer Data stored on ROSALIND's equipment or in ROSALIND's facilities, or any unauthorized access to any facilities or equipment resulting in loss, disclosure, or alteration of any Customer Data, or any actual loss of or suspected threats to the security of Customer Data, ROSALIND personnel will immediately:

a) notify Customer's Information Security Department of the incident;
b) investigate and provide assistance in the investigation of the security incident by conducting a through root-cause analysis, producing a report of such analysis and providing such report to Customer;
c) provide Customer with detailed information about the security incident;
d) take all commercially reasonable steps to mitigate the effects of the security incident and providing a report of such mitigation efforts to Customer; and
e) implement a remediation plan and monitor the resolution of breaches and vulnerabilities related to Customer Data to ensure that appropriate corrective action is taken on a timely basis.

7. Reporting

ROSALIND shall provide a preliminary report of all issues related to security breaches to Customer's Information Security department within 24 hours after discovery and a final report promptly upon completion of investigation. ROSALIND shall provide prior notice to Customer of any proposed communications to third parties related to any security incident and will work on them in coordination with Customer. ROSALIND shall not issue any communication without Customer's approval unless required by applicable law.

8. Backup and Archives

ROSALIND shall back up, archive, and maintain duplicate or redundant systems that can fully recover all Customer Data on a daily basis. ROSALIND shall establish and follow procedures and frequency intervals for protecting customer data.

9. Confidentiality and Compliance

Customer shall maintain the confidentiality of the reports it reviews. Customer shall comply with all applicable laws and regulations, including to the Fair Credit Reporting Act and data protection and privacy regulations when acting pursuant to this Agreement.

10. Network Security
ROSALIND shall configure its network infrastructure to enforce the "principle of least access," including filters that allow only the minimum required traffic.

11. Host Monitoring
Upon written request, ROSALIND shall disclose the high level processes for monitoring the integrity and availability of the hosts.

12. Passwords
ROSALIND shall store any passwords within a secured database server, using industry standard security measures behind OnRamp's firewall. ROSALIND shall use SHA-256 or higher to scramble or hash the database password. ROSALIND's system must require this password upon application startup to connect to the database.

13. Web Security
ROSALIND shall provide Customer with the process for doing quality assurance testing for the application, for example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the architecture.

14. Encryption Algorithms
ROSALIND shall use cryptographic algorithms that have been published and evaluated by the general cryptographic community. ROSALIND shall use encryption algorithms that are sufficient strength to equate to 256-bit or better. ROSALIND may use hashing functions SHA-256 or higher. ROSALIND shall not use any "homegrown" cryptography, such as symmetric, asymmetric, or hashing algorithm.

15. Encryption Key Management
ROSALIND shall provide encryption key management. ROSALIND shall protect private keys in storage, transit, and backup. A separate key per customer is preferred instead of a global key for all customers. ROSALIND shall segregate the encryption key and encryption key management process from any hosts that store and process the data. ROSALIND shall provide Customer with documentation of its security controls for the secure key management. ROSALIND shall provide an effective key destruction technique, such as crypto shredding, to ensure that the encryption keys are destroyed and unrecoverable after the Agreement is terminated.

16. Identity Provisioning and De-provisioning
ROSALIND shall provide a secure and timely management of on-boarding and off-boarding of cloud service users.

17. Strong Authentication
ROSALIND shall use two-factor authentication and certificates to authenticate their remote administrators who manage their cloud services, or an alternative strong authentication method.

18. Authorization and Access Controls
ROSALIND shall maintain a policy and role-based access control model to log user access information for compliance audit and incident investigation purposes.