Security Standards

Solvemate will abide by the security standards set forth below (“**Security Standards**”), which detail the various actions taken by Solvemate to provide the Solvemate Services (“**Information Security**”). During the Subscription Term, these Security Standards may change without notice, as standards evolve or as additional controls are implemented or existing controls are modified as deemed reasonably necessary by Solvemate, provided that such changes will not bring the Security Standards below industry standard security measures.

Definitions

Terms not defined herein will have the meanings ascribed to them in the relevant agreement for the Solvemate Services entered into between the parties.

1 Risk Management.

- An annual Information Security risk assessment is performed covering Solvemate facilities and information assets.
- The risk assessment is conducted using an industry standard methodology to aid in identifying, measuring, and treating known risks.
- Risk assessment results and risk mitigation suggestions are shared with the executive management team.
- The risk assessment results will specify proposed changes to systems, processes, policies, or tools, in order to reduce security vulnerabilities and threats, if any.

2. Security Policy.

- Policies, including those related to data privacy, security and acceptable use, are assessed and approved by Solvemate senior management. Policies are documented and published among all relevant personnel.
- Employees and contracted third parties are required to comply with Solvemate policies relevant to their scope of work.
- New employees attend new hire training, which includes training modules on confidentiality obligations, information security, compliance, and data protection.
- Employees attend annual Information Security training, which covers Solvemate Information Security policies and expectations.
- Where required, policies are supported by associated procedures, standards, and guidelines.
- Information Security policies are updated, as needed, to reflect changes to business objectives or risk.

- Senior management performs an annual review of all Information Security policies.
- Information Security policies are stored, maintained, updated, and published in a centralized location accessible to employees and third parties.
- Solvemate's employee handbook contains sections on password requirements, Internet usage, computer security, confidentiality, social media, customer data protection, and Company data protection.

3. Organization of Information Security.

- Information Security governance and data protection compliance for the Company are the responsibility of Solvemate's Chief Technical Officer.
- Confidentiality and non-disclosure agreements are required when sharing sensitive, proprietary personal or otherwise confidential information between Solvemate and a third-party.

4. Asset Management.

- Solvemate desktops and laptops utilize encrypted storage partitions.
- Solvemate maintains a data and media management policy that covers the disposal of electronic assets and associated media.

5. Human Resources Information Security.

- Security roles and responsibilities for employees are defined and documented.
- Solvemate performs reasonable background screening of applicants, including job history and references (each subject to local laws).
- Solvemate requires all new employees to sign employee agreements, which include comprehensive non-disclosure and confidentiality commitments.
- Solvemate maintains a formal information security awareness and training program that includes new hire training and annual developer secure code training.
- Information Security awareness is enhanced through regular communications using Solvemate's internal social media tool and company-wide emails, as necessary.
- The organization maintains attendance records for formal security awareness training sessions.
- Employees with responsibility for Information Security participate in additional training on security protection techniques, risks, and latest trends.
- The Human Resources department notifies Information Technology and Operations Teams of changes in employment status and employment termination.
- Solvemate maintains a documented procedure for changes in employment status and employment termination (including notification, access modification, and asset collection). New third-party service providers whose services involve access to any

confidential information must agree contractually to data privacy and security commitments commensurate with their access and handling of confidential information.

6. Physical and Environmental Security.

- Physical security controls in all data centers utilized by Solvemate, in providing the service, include protection of facility perimeters using various access control measures (including supervised entry, 24/7/365 on-premise security teams, CCTV systems).
- Access to data centers is limited to authorized employees or contractors only.
- Controls are in place to protect against environmental hazards at all data centers.
- All data center facilities have successfully been attested to SSAE 16 SOC 2 type 2, ISO 27001, or similar requirements.
- Solvemate office space is secured from visitor access except for areas staffed by reception or security personnel.
- the office space is equipped with an alarm system that is connected to a security company that is 24/7/365 on standby.

7. Communications and Operations Management.

- The operation of systems and applications that support the Solvemate Services are subject to documented operating procedures.
- The operations team maintains hardened standard server configurations. Systems are deployed and configured in a uniform manner using configuration management systems.
- Solvemate maintains change control programs for development, operations, and Information Technology teams.
- Separate environments are maintained to allow for the testing of changes.
- The organization maintains documented backup procedures. Full backups are performed daily for all production databases. Customer Content backups are transferred to an offsite location and stored encrypted for at least 30 days.
- All systems and network devices are synchronized to a reliable/ and accurate time source via the "Network Time Protocol" (NTP)
- All servers are configured to log authorized access, privileged operations (administrator actions), and unauthorized access attempts.
- All servers are logging executed commands via the sudo utility.
- Log files are transmitted to and stored in a separate log server to protect against modification or loss.

- All event-alerting tools escalate into pager notifications for the 24x7 incident response teams, providing Operations, Network Engineering, and the Security teams, as needed.

8. Access Controls.

- Solvemate maintains an access control policy that outlines requirements for the use of user IDs and passwords.
- The organization publishes and maintains a password management standard. This standard enforces a minimum length of 8 characters and special characters.
- Generic accounts are prohibited for user access. Access to the “root” account is restricted to Operations personnel deemed necessary.
- All access to the back-end servers and network infrastructure requires authentication based on individual SSH key pairs.
- All access controls are based on “least privilege” and “need to know” principles.
- Upon notice of termination of Solvemate personnel, all user access is removed. All critical system access is removed immediately upon notification.

9. Information Systems Acquisition, Development, and Maintenance.

- Product features are managed through a formalized product management process. Security requirements are discussed and formulated during scoping and design discussions.
- Solvemate maintains engineering resources whose primary responsibility is identifying and remediating bugs found in the Solvemate Service.
- Source code repositories are scanned regularly by a static analysis / code quality tool. Any security issues are validated, risk ranked, and placed in a dedicated bug tracking system for remediation.
- Solvemate also communicates application security vulnerabilities and mitigation approaches during regular brown bag meetings.
- Solvemate utilizes framework security controls to limit exposure to common application security risks, including cross-site scripting (XSS), cross-site request forgery (CSRF), and SQL injection (SQLi).
- Solvemate maintains QA resources dedicated to reviewing and testing application functionality and stability.
- Solvemate performs third-party security audits using a variety of vendors.
- Solvemate maintains a "Responsible Disclosure Policy" that provides an avenue for security researchers to submit vulnerabilities to the Information Security group for remediation.

- Application source code is stored in a central repository. Access to source code is limited to authorized individuals.
- Changes to Solvemate software are tested before production deployment. Deployment processes include unit testing at the source environment, as well as integration and functional testing within a test environment prior to implementation in production.
- Solvemate follows change control procedures for all system and software configuration changes. These controls include, at a minimum, a documented impact for each change, change review, testing of operational functionality, and back-out procedures.
- Customer Content is not used in testing environments.
- Emergency fixes are pushed to production, as needed. Change management is retrospectively performed.
- Customer Content is stored in a shared database environment with other customers. Account identifiers are used to distinguish data for different customers. Application security controls limit a Customer being able to access another Customer's data or content.

10. Information Security Incident Management.

- Solvemate maintains an incident response process that includes direct participation and cooperation between support, security, and operations teams.
- The Solvemate incident response process includes notification, escalation, and reporting. When required, Customer notification is initiated through the Solvemate status page, Twitter notifications, Solvemate initiated reporting tickets, or direct email/phone communication to account contacts.
- Internally, Solvemate maintains an incident response plan that is tested on a regular basis. The plan addresses specific incident response procedures, data backup procedures, roles and responsibilities, customer communication, contact strategies, and legal and shareholder information flow.
- The incident response plan is tested on a regular basis, at least annually.
- Solvemate has relationships with third-party vendors to assist with forensics and investigations, as necessary.