Aera Security & Privacy Documentation

1. Commitment to Security & Privacy and Scope

Aera is committed to providing a comprehensive security and privacy program that carefully considers data protection matters across our suite of products and services, including data submitted by customers to our Service ("Customer Data"). Aera utilizes infrastructure-as-a-service cloud providers as further described in the Agreement and/or Documentation (each, a "**Cloud Provider**") and provides the Service to Customer using a VPC/VNET and storage hosted by the applicable Cloud Provider (the "**Cloud Environment**").

2. Scope

This documentation describes the security-related audits and certifications received for, and the administrative, technical, and physical controls applicable to, the Aera cloud based services ("Service(s)"). This documentation does not apply to free evaluation services or Aera Developer made available by Aera.

3. Permitted Purposes

Aera will use Customer Data only as follows:

3.1 **Privacy**. Aera has implemented procedures designed to ensure that Customer Data is processed only as instructed by the Customer through the entire chain of processing activities by Aera and its subcontractors may use only the Customer Data necessary to perform the Service under the Agreement.

3.2 **Sale or other transfer prohibited**. Aera will not transfer, sell, or otherwise distribute or make any Customer Data available to any third party except as otherwise specifically provided under the Agreement.

4. Information Security Requirements

4.1 **General security requirement**. Aera will maintain physical, administrative, and technical safeguards appropriate to (a) the size, scope and type of Aera's business; (b) the amount of resources available to Aera; (c) the type of information that Aera will store and process; and (d) the need for security and protection from unauthorized disclosure of such Customer Data, and consistent with industry-accepted best practices [(including the International Organization for Standardization's standards ISO 27001 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework, or other similar industry standards for information security)] to protect the confidentiality, integrity, and availability of Customer Data.

4.2 **Specific safeguard requirements**. In addition to following the above standards, Aera's information security program will include, at a minimum, the following safeguards and controls:

4.2.1 **Written information security program**. Aera will implement a written information security program, including appropriate policies, procedures, and risk assessments that are reviewed at least annually.

4.2.2 **Security awareness training; Background Checks; Confidentiality; Disciplinary Policy**. Aera will provide periodic security training to its employees on relevant threats and business requirements such as social-engineering attacks, sensitive data handling, causes of unintentional data exposure, and security incident identification and reporting. Aera performs background checks on any employees who are to perform material aspects of the Service or have access to Customer Data. Aera requires all personnel to acknowledge in writing, at the time of hire, that they will comply with its information and security management program and protect all Customer Data at all times. Aera maintains a disciplinary policy and process in the event Aera personnel violate the information and security management program.

4.2.3 **Data inventory**. Aera will document and maintain information regarding how and where Customer Data is processed while in Aera's possession or control.

4.2.4 **Secure configurations**. Aera will manage security configurations of its systems on the Cloud Environment using industry standard practices to protect Customer Data from exploitation through vulnerable services and settings.

4.2.5 **Controlled use of administrative privileges**. Aera will limit and control the use of administrative privileges on the Cloud Environment consistent with industry standard practices.

4.2.6 **Vulnerability and patch management**. Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to the Service. Upon becoming aware of such vulnerabilities, Aera will use commercially reasonable efforts to address critical and high vulnerabilities within 30 days, and medium vulnerabilities within 90 days. To assess whether a vulnerability is 'critical', 'high', or 'medium', Aera leverages the National Vulnerability Database's (NVD) Common Vulnerability Scoring System (CVSS), or where applicable, the U.S.-CERT rating.

4.2.7 **Monitoring**. Monitoring tools or services, such as host-based intrusion detection tools, are utilized to log certain activities and changes within the Cloud Environment.

4.2.8 **Malware defenses**. Aera will employ then-current industry-standard measures to test the Service to detect and remediate viruses, Trojan horses, worms, logic bombs, or other harmful code or programs designed to negatively impact the operation or performance of the Service. Aera does not monitor Customer Data for Malicious Code.

4.2.9 **Firewalls**. Aera will protect the Cloud Environment using industry standard firewall or security group technology to deny-all default policies to prevent egress and ingress network traffic protocols other than those that are business required.

4.2.10 **Change Management**. Aera maintains a documented change management program for the Service.

4.2.11 **Hardening**. The Cloud Environment shall be hardened using industry-standard practices to protect it from vulnerabilities, including by changing default passwords, removing unnecessary software, disabling or removing unnecessary services, and regular patching.

4.2.12 **Encryption**. Aera will encrypt all Customer Data at rest and when in transit across open networks in accordance with industry best practices. Upon Customer's written request, the supplier will confirm that all copies of encryption keys have been securely deleted.

4.2.13 **Access controls**. Aera will implement the following access controls with respect to Customer Data:

(a) **Unique IDs**. Aera will assign individual, unique IDs to all personnel with access to Customer Data, including accounts with administrative access. Accounts with access to Customer Data will not be shared.

(b) **Need-to-know**. Aera will restrict access to Customer Data to only those personnel with a "need-to-know" for a permitted purpose.

(c) **User access review**. Aera will periodically review personnel and services with access to Customer Data and remove accounts that no longer require access. This review will be performed at least once every 180 days.

4.2.14 **Disaster Recovery.** Aera maintains policies and procedures for responding to an emergency or a Force Majeure Event that could damage Customer Data or production systems that contain Customer Data. Such procedures include:

a) Data Backups: A policy for performing periodic backups of production file systems and databases;

b) Disaster Recovery: A formal disaster recovery plan for the production environment designed to minimize disruption to the Service, which includes requirements for the disaster plan to be tested on a regular basis;

c) Business Continuity Plan: A formal process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

4.2.15 **Account and password management**. Aera will implement the following account and password management policies to protect access to the Cloud Environment:

(a) **No default passwords**. Before deploying any new hardware, software, or other asset, Aera will change all default and manufacturer-supplied passwords to a password consistent with the password strength requirements in subsection (c).

(b) **Inventory of administrative accounts**. Aera will maintain an inventory of all administrator accounts with access to Customer Data.

(c) **Password strength**. Aera will use strong passwords by enforcing the following minimum requirements:

- passwords must be a minimum length of 8 characters;
- passwords may not match commonly used, expected, or compromised passwords; and
- Aera will force a password change if there is evidence the password may have been compromised.

(d) **Credential encryption**. Encrypted passwords and other secrets shall be stored in an industry-accepted form that is resistant to offline attacks.

(e) **Rate limiting**. Aera will implement an industry-accepted rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on a user's account.

4.2.16 **Remote access; multi-factor authentication**. Aera will implement multi-factor authentication (i.e., requiring at least two factors to authenticate a user) for remote access to the Cloud Environment containing Customer Data.

4.2.17 **Data segregation**. Except where expressly authorized by Customer in writing, Aera will logically isolate Customer Data in the Cloud Environment at all times from Aera's and any third-party data.

4.2.18 **Security testing**. Aera will conduct periodic internal and external penetration testing of systems that process Customer Data to identify vulnerabilities and attack vectors that can be used to exploit those systems. Identified vulnerabilities shall be addressed as part of Aera's vulnerability management program.

5. Data Retention, Return, and Destruction

5.1 **Retention**. Aera will retain Customer Data only as necessary for the permitted purposes.

5.2 **Return and secure deletion of Customer Data**. At any time during the Term at Customer's request, or upon the termination or expiration of the Agreement for any reason, Aera shall securely delete all copies of Customer Data in its possession or control. Supplier shall confirm in writing that all copies of Customer Data have been securely deleted.

5.3 **Archival copies**. If Aera retains archival copies of Customer Data for any purposes, Aera shall (i) not use the archived Customer Data for any other purpose; and (ii) remain bound by its obligations under this exhibit, including, but not limited to, its obligations to protect the information using appropriate safeguards and to notify Customer of any Security Incident involving such Customer Data.

5.4 **Deletion standard**. All Customer Data deleted by Supplier will be securely deleted using an industry-accepted practice designed to prevent data from being recovered using standard disk and file recovery utilities (e.g., secure overwriting, degaussing of magnetic media in an electromagnetic flux field of 5000+ GER, shredding, or mechanical disintegration). With respect to Customer Data encrypted in compliance with this security policy, Aera may delete data by permanently and securely deleting all copies of the encryption keys.

6. Security Reviews and Audits

Aera provides its customers, upon their request, with a copy of Aera's then-current audit report, including information as to whether the security audit revealed any material findings in the Service; and if so, the nature of each finding discovered.

7. Security Incidents

7.1 **Security Incident defined**. A "Security Incident" is any actual and verified unauthorized access to, or use of Customer Data.

7.2 **Incident response plan**. Aera will maintain a written incident response plan and make available a copy of the plan to Customer upon request. Supplier will remedy each Security Incident in a timely manner following its response plan and industry best practices.

7.3 **Notice required**. Aera will notify Customer of any Security Incident within 72 hours of becoming aware of the Security Incident.

7.4 **Cooperation with Customer**. Aera will cooperate with an impacted customer's reasonable request for information regarding such Security Incident, and Aera will provide regular updates on any such Security Incident and the investigative action and corrective action(s) taken Aera. Communications by or on behalf of Aera with Customer in connection with a Security Incident shall not be construed as an acknowledgment by Aera of any fault or liability with respect to the Security Incident.

7.5 **Third-party notifications**. Aera agrees that, unless as legally required, it shall not notify any third party of any Security Incident affecting only Customer's Customer Data without first obtaining Customer's prior written consent.

8. Notice of Legal Process

Supplier will, to the extent allowed under applicable law, inform Aera when Customer Data is being sought in response to legal process or other applicable law (e.g., 18 U.S.C. § 2705(b)).

9. Communication with Users

Separate from and as a complement to the Service, Aera may provide Users access to online communities that provide technical support resources and communicate with Users from time to time, and also send announcements and details about Aera's products, services, industry events, professional certifications, and other relevant information that Users may find useful.

10. Shared Security Responsibilities. Without diminishing Aera's commitments in this Security & Privacy Documentation, Customer agrees:

10.1. Aera has no obligation to assess the content, accuracy or legality of Customer Data, including to identify information subject to any specific legal, regulatory or other requirement and Customer is responsible for making appropriate use of the Service to ensure a level of security appropriate to the particular content of Customer Data, including, where appropriate, implementation of encryption functionality, such as the "tri-secret secure" feature, pseudonymization of Customer Data, and configuration of the Service to back-up Customer Data;

10.2. Customer is responsible for managing and protecting its User roles and credentials, including but not limited to (i) ensuring that all Users keep credentials confidential and not share such information with unauthorized parties, (ii) promptly reporting to Aera any suspicious activities related to Customer's account (e.g., a user credential has been compromised) by submitting a support ticket and designating it as a Severity Level 1 in accordance with the Support Policy, (iii) appropriately configuring User and role-based access controls, including scope and duration of User access, taking into account the nature of its Customer Data, and (iv) maintaining appropriate password uniqueness, length, complexity, and expiration;

10.3. To appropriately manage and protect any Customer-managed encryption keys to ensure the integrity, availability, and confidentiality of the key and Customer Data encrypted with such key; and

10.4. To promptly update its On-Premise Components whenever Aera announces an update.