Data Security Notice

This Data Security Notice describes the technical and organisational measures Serene Health Limited ("Serene") maintains to protect its systems, services and customer data. It forms part of Serene's Information Security Management System (ISMS).

Serene maintains a documented information security programme aligned with ISO 27001 and implements appropriate administrative, organisational and technical measures designed to protect the confidentiality, integrity and availability of information under its control.

1. Deployment Model

Serene operates a cloud-based technology environment using approved cloud service providers. Serene maintains documented architecture and security controls designed to protect its systems and customer data.

Production environments are logically separated from development and testing environments, and access is restricted in accordance with role-based access controls and the principle of least privilege.

2. Client Content

Serene primarily processes pseudonymised customer data in accordance with the applicable client agreement, Statement of Work and Data Processing Agreement.

Customer data is protected through appropriate technical and organisational measures, including encryption, access controls, authentication, logging and monitoring.

Customer data is retained and deleted in accordance with Serene's Data Retention Policy and applicable contractual requirements.

3. Serene Audits & Certifications

Serene has an established system of internal controls to monitor its security programme and ensure compliance with recognised industry best practice and standards.

Serene uses independent third-party auditors to assess the Serene Security Programme at least annually as part of its ongoing certification to ISO 27001.

4. Administrative Controls

4.1 Governance

Serene's senior management oversees the Information Security Management System, with defined responsibilities for information security assigned across the organisation. Relevant policies are reviewed and approved in accordance with Serene's governance framework.

4.2 Change Management

Serene maintains a documented change management policy, reviewed annually, which includes but is not limited to, evaluating changes of or relating to systems authentication.

4.3 ISMS; Policies and Procedures

Serene has implemented a formal Information Security Management System ("**ISMS**") in order to protect the confidentiality, integrity, authenticity, and availability of Serene' data and information systems, and to ensure the effectiveness of security controls over data and information systems that support operations.

The Serene Security Programme implemented under the ISMS includes a comprehensive set of privacy and security policies and procedures developed and maintained by the security, legal, privacy, and information security teams ("**Security Policies**").

The Security Policies are aligned with information security standards (such as ISO 27001) and cover topics including but not limited to: security controls when accessing Serene Services and Systems; confidentiality of Customer Content;

acceptable use of company technology, systems and data; processes for reporting security incidents; and privacy and security best practices. The Security Policies are reviewed and updated annually.

4.4 Employee Training

Employees receive comprehensive training on the Security Policies upon recruitment and refresher training are given annually. Employees are required to certify and agree to the Security Policies and Employees who violate the Security Policies are subject to disciplinary action, including warnings, suspension and up to (and including) termination.

4.5 Employees Screening and Evaluation

Serene undertakes appropriate pre-employment screening, proportionate to the role and permitted by applicable law. Employees and contractors are subject to appropriate confidentiality obligations.

4.6 Monitoring & Logging

Serene employs monitoring and logging technology to help detect and prevent unauthorised access attempts to its network and equipment.

4.7 Access Review

Active users with access to the Systems and Services are reviewed at least quarterly and are promptly removed upon termination of employment. As part of the Employees offboarding process, all accesses are revoked and data assets are securely wiped.

4.8 Third Party Risk Management

Serene assesses the security compliance of applicable third parties, including vendors and sub-processors, in order to measure and manage risk. This includes, but is not limited to, conducting a security risk assessment and due diligence prior to engagement and reviewing external audit reports from critical vendors at least annually. In addition, applicable vendors and sub-processors are required to sign a data processing agreement that includes compliance with applicable data protection laws, as well as confidentiality requirements.

5. Systems & Network Security

5.1 Platform Controls

5.1.1 Isolation

Serene leverages multiple layers of network security controls, including network-level isolation, for separation between the Serene Control Plane and Customer Data Plane, and between Workspaces within the Serene Data Plane.

5.1.2 Firewalls & Security Groups

Firewalls are implemented as network access control lists or security groups within the Cloud Service Provider's account. Serene also configures local firewalls or security groups within the Customer Data Plane.

5.2 Hardening

Serene employs industry standards to harden images and operating systems under its control that are deployed within the Platform Services, including deploying baseline images with hardened security configuration such as disabled remote root login, isolation of user code, and images are regularly updated and refreshed.

For Systems under Serene control supporting the production data processing environment, Serene tracks security configurations against industry standard baselines such as CIS and STIG.

5.3 Encryption

5.3.1 Encryption of data-in-transit

Customer Content is encrypted using cryptographically secure protocols (TLS v.1.2 or higher) in transit between (1) Customer and the Serene Control Plane and (2) the Serene Control Plane and the Data Plane. Additionally, depending on functionality provided by the Cloud Service Provider, Customers may optionally encrypt communications between clusters within the Data Plane

5.3.2 Review

Cryptographic standards are periodically reviewed and selected technologies and ciphers are updated in accordance with assessed risk and market acceptance of new standards.

5.3.3 Customer Options; Responsibilities

Customers may choose to leverage additional encryption options for data in transit within the Customer Data Plane or Serene Data Plane as described in the Documentation. Customer shall, based on the sensitivity of the Customer Content, configure the Platform Services and Customer Systems to encrypt Customer Content where appropriate.

5.4 Monitoring & Logging

5.4.1 Intrusion Detection Systems

Serene leverages security capabilities provided natively by Cloud Service Providers for security detection.

5.4.2 Generation

Serene generates audit logs from Customer's use of the Platform Services. The logs are designed to store information about material events within the Platform Services.

5.4.3 Integrity

Serene stores audit logs in a manner designed to protect the audit logs from tampering.

4.5.4 Retention

Serene stores audit logs for at least one year.

5.5 Penetration Testing

Serene conducts third-party penetration tests at least annually, employs in-house offensive security Employees, and also maintains a public bug bounty programme.

5.6 Vulnerability Management & Remediation

Serene regularly conducts authenticated scans on representative hosts within the SDLC pipeline to identify vulnerabilities and emerging security threats that could affect the Data Plane and Serene Control Plane. Serene will make commercially reasonable efforts to address critical vulnerabilities within 14 days, high-severity vulnerabilities within 30 days, and medium-severity vulnerabilities within 60 days.

These timeframes are measured from the date that a compatible, vendor-supplied patch becomes available for publicly declared third-party vulnerabilities, or from the date the vulnerability is confirmed for internal vulnerabilities.

5.7 Patching

5.7.1 Control Plane

Serene deploys new code to the Serene Control on an ongoing basis.

5.8 Corporate Controls

5.8.1 Access Controls

- **Authentication:** Serene Employees are authenticated through single sign-on (SSO), 802.1x (or similar) where applicable, and use a unique user ID and password combination and multi-factor authentication. Privileges are consistent with least privilege principles. Security Policies prohibits Employees from sharing or reusing credentials, passwords, IDs, or other authentication information.

- **Role-Based Access Controls (RBACs):** Only authorised roles are allowed to access systems processing customer and personal data. Serene enforces RBACs (based on security groups and access control lists) and restricts access to Customer Content based on the principle of 'least privilege' and segregation of responsibilities and duties.

5.8.2 Pseudonymisation

Information stored in activity logs and databases are protected where appropriate using a unique randomised user identifier to mitigate risk of re-identification of data subjects.

5.8.3 Workstation Controls

Serene enforces certain security controls on its workstations used by Employees, including:

- Full-disk encryption
- Anti-malware software
- Automatic screen lock after 15 minutes of inactivity
- Secure VPN

6. Incident Detection & Response

6.1 Detection & Investigation

Serene deploys and develops intrusion detection monitoring across its computing resources, with alert notifications sent to the designated incident response personnel for triage and response. The designated incident response personnel employ an incident response framework to manage and minimise the effects of unplanned security events.

6.2 Security Incidents; Security Breaches

"**Security Breach**" refers to any breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Data under Serene's control.

A "**Security Incident**" is any actual or attempted breach of security that does not reach the level of a Security Breach.

A Security Breach does not include unsuccessful attempts or activities that do not compromise the security of Customer Data. This includes, but is not limited to, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing, or other unauthorised access to traffic data that does not result in access beyond headers.

Serene maintains a record of known Security Incidents and Security Breaches, which includes descriptions, dates and times of relevant activities, and the disposition of the incident.

Suspected and confirmed Security Incidents are investigated by security, operations, or support employees, and appropriate resolution steps are identified and documented.

For any confirmed Security Incidents, Serene will take appropriate and reasonable steps to minimise product and customer damage or unauthorised disclosure. All incidents are logged in an incident tracking system, which is subject to annual auditing.

6.3 Communications & Cooperation

In accordance with applicable data protection laws, Serene will notify Customer of a Security Breach for which that Customer is impacted without undue delay after becoming aware of the Security Breach, and take appropriate measures to address the Security Breach, including measures to mitigate any adverse effects resulting from the Security Breach.

7. Backups, Business Continuity, and Disaster Recovery

Serene maintains documented Business Continuity and Disaster Recovery procedures which are reviewed and tested periodically.

Appropriate backup and resilience measures are maintained for systems and data under Serene's control, taking into account system criticality and applicable contractual requirements.

Backup, recovery and resilience arrangements are documented and periodically reviewed.

8. Data Deletion

Customer data is retained in accordance with the applicable client contract, Statement of Work and/or Data Processing Agreement and Serene's Data Retention Policy.

At the end of the applicable retention period, customer personal data is securely deleted, returned or anonymised in accordance with applicable contractual requirements.

9. Secure Software Development Lifecycle (“SDLC”)

9.1 Security Design Review

Feature designs are assessed by security Employees for their security impact to the Serene Platform, for example, additions or modifications to access controls, data flows, and logging.

9.2 Security Training

Architects are required to take Secure SDLC training.

9.3 Change Control

Serene' controls are designed to securely manage assets, configurations, and changes throughout the SDLC.

9.4 Code Scanning

Static and dynamic code scans are regularly run and reviewed.

9.5 Penetration Testing

As part of the Security Design Review process, certain features are identified and subjected to penetration testing prior to release.

9.6 Code Approval

Functional owners are required to approve code in their area of responsibility prior to the code being merged for production.

9.7 Multi-Factor Authentication

Accessing the Serene code repository requires Multi-Factor Authentication.

9.8 Code Deployment

Production code is deployed via automated continuous integration / continuous deployment pipeline processes. The release management teams are separated from the engineering teams that build the product.

9.9 Production Separation

Serene separates production Platform Services Systems from testing and development Platform Services Systems.

10. Certificates

ISO and all other certificates are provided upon request and as part of any auditing process.

Version Control

Title	Data Security Notice (PC-5)
Description	Notice Document
Created By	Information Security Office
Date Created	2025
Maintained By	Information Security Office

Approved By	Board of Directors			
Version Number	**Modified By**	**Modifications Made**	**Date Modified**	**Status**
1.0	ISO	Initial creation	2024	Live
2.0	ISO	Reviewed for 2025 Audit purposes	04/2025	Live
2.1	ISO	Reviewed for 2026 Audit purposes - wording updates to reflect operating model	04/2026	Live