

Service Definition

Service name: Snapshot AI

Supplier: Vesper Software Limited

1. Service overview

Snapshot AI is a cloud-based software service that provides engineering leaders with insight into software delivery activity by analysing data from development and delivery tools. The service supports visibility, risk identification, and informed decision-making across engineering teams.

2. Service scope

The service ingests data from supported third-party systems via APIs and presents insights through a secure web interface. Snapshot AI is provided as a fully managed Software as a Service (SaaS) offering.

3. Onboarding and offboarding

Onboarding is delivered remotely and includes configuration, integrations, and user setup. Optional onsite onboarding can be provided by agreement. Offboarding includes customer data export in standard formats and secure deletion of customer data following contract termination.

4. Service availability and support

Snapshot AI targets 99.5% availability per calendar month, excluding planned maintenance. Support is provided via email and phone during business hours. Enhanced support options, including dedicated account management and additional technical support, are available at additional cost.

5. Data backup, restore, and resilience

Customer data is backed up regularly using cloud-provider managed backup services. The service is hosted on resilient infrastructure deployed across multiple availability zones to reduce single points of failure.

6. Maintenance and outages

Planned maintenance is scheduled outside core business hours where possible. Customers are notified in advance of planned maintenance and informed of service-impacting incidents via email.

7. Hosting and data location

Snapshot AI is hosted on third-party cloud infrastructure. Data residency requirements can be agreed contractually and configured by the supplier where required.

8. Security

Snapshot AI operates an information security management system aligned with ISO/IEC 27001 and SOC 2 Type II. Security controls include encryption of data in transit and at rest, access control, monitoring, vulnerability management, and incident response processes.

9. Access to data and audit

Customers can request access to audit and activity information relating to their use of the service through the support team. Audit logs are retained for at least 12 months.

10. Technical requirements

Users require a modern web browser and internet connectivity to access the service. No local installation or specialist software is required.

11. Accessibility

The service is accessed via a browser-based interface designed with accessibility considerations in mind. This document is provided in an accessible format suitable for screen readers when exported as PDF/A.