



Speech Enabled Visual Assistance (SEVA) Service Definition Document

What the service is:

SEVA Software & Support Services

SEVA is a software solution licensed to resellers along with defined support and service components. This document describes the scope of services provided by Purview Technology during the license term.

Service description: SEVA is an AI-enabled software platform designed to run on supported smart glasses and companion devices, and to integrate with customer systems via APIs. It enables voice-driven, hands-free and guided workflows for end users, while providing administration and reporting capabilities for the Licensee/reseller.

Who it is for: SEVA is licensed to resellers (Licensees) who deploy it to their end customers and users. Typical use cases include hands-free field operations, inspections, assistance scenarios, and other guided workflows where smart-glasses based interaction adds productivity or accessibility value.

How it works in practice: The Licensee provisions users, configures workflows and integrations, and deploys SEVA on supported devices. End users sign in, follow guided prompts, and interact through voice commands and on-device UI. Data generated within SEVA (e.g., workflow status, captured media, and logs) is synchronised and/or exchanged with the Licensee's systems through supported APIs and integrations (subject to configuration).

Key features and benefits (subject to configuration): Hands-free, voice-driven operation - Smart glasses optimised UX for guided workflows - Configurable user roles and permissions - API support for integration with customer platforms - Ongoing upgrades during the license term (bug fixes, performance improvements, and new features).

Limitations and exclusions: Hardware procurement, replacement, and device warranty are excluded - Network/internet availability is the Licensee's responsibility - Third-party service outages (e.g., telephony, identity providers) are outside Purview Technology control - End-user adoption support for smart glasses is excluded unless separately contracted - Customisations are subject to agreed scope and technical feasibility.

Services Included

Initial Setup Support

Purview Technology will provide initial set-up support to the reseller trainer to assist with installation and configuration of the SEVA software. This includes guidance to ensure the software operates correctly within the Licensee's environment.



API Supporting Services

Purview Technology will provide support for the software's Application Programming Interface (API), enabling seamless integration with the Licensee's systems.

Software Upgrades

During the active license period, the Licensee will receive free software upgrades, including: - Bug fixes - Performance improvements - new features and functionalities.

Any costs related to API usage or third-party call features during the license period are included.

Technical Support (L2 & L3)

Purview Technology will provide Level 2 (L2) and Level 3 (L3) technical support for software-related issues during the license term.

Reseller Responsibility: Level 1 (L1) help desk and end-user support - Routing validated software issues to the Purview Technology support team.

L2 Support Includes: - Software issue diagnosis - Configuration issues - Software functionality queries.

L3 Support Includes: - Advanced technical troubleshooting and debugging - System-specific or integration issues - Customisation assistance - Software patches for identified bugs
Hardware-related issues and user adoption support for smart glasses are excluded.

Support Duration & SLA

- Ticket acknowledgement SLA: within 24 hours
- Resolution timelines: up to 5 working days depending on severity

Support is available for the full duration of the active license period from the date of purchase.

• Service Levels

Availability target (Purview-hosted): 99.5% monthly service availability, excluding planned maintenance and force majeure events.

Support hours (standard): Monday to Friday, 09:00-18:00 IST, excluding public holidays. Enhanced 24x7 coverage for critical incidents can be provided under an optional support package.

Performance expectations: Target API responsiveness and UI performance will be maintained under normal operating loads. Specific throughput/latency targets can be agreed based on sizing and usage profiles.

Response targets by severity (standard): Severity 1 (Critical: service unavailable or major security incident): acknowledge within 4 hours, continuous work until service restored during support hours - Severity 2 (High: major feature impaired, workaround limited): acknowledge within 1 business day, target fix/workaround within 3 business days - Severity 3 (Medium: limited impact, workaround available): acknowledge within 1 business day, target fix in planned release - Severity 4 (Low: questions/minor defects): acknowledge within 2 business days.

Escalation path: L1 (Reseller) -> Purview L2 Support -> Purview L3 Engineering -> Engineering Lead/Management (as required).



• After Sales Support & Customer Success

Ongoing support includes: Account management for renewals, licensing queries, and commercial coordination - Customer success check-ins (as agreed) to review usage, issues, and upcoming needs - Change and release communications (release notes, planned maintenance advisories, and important updates) shared via agreed channels (e-mail and/or ticketing system).

Optional enhanced support packages (on request): 24x7 Severity 1 coverage - Dedicated support contact and faster response SLAs - Proactive monitoring and periodic health checks - On-site/remote enablement sessions for new deployments or major releases.

• Data Backup, Restore and Disaster Recovery

Applicability: The following applies to Purview-hosted deployments. For customer-hosted/on-premises deployments, the Licensee is responsible for backup, restore, and disaster recovery unless separately contracted.

Backups: Database and configuration data are backed up using automated mechanisms - Backups are encrypted and access-controlled - Backup retention follows a rolling retention policy (e.g., daily backups retained for at least 30 days), unless otherwise agreed.

Backup frequency: Daily automated backups (minimum) - More frequent backups (e.g., hourly snapshots) can be enabled for specific tiers or critical environments by agreement.

Restore process & timelines: Restore requests are raised via support ticket - Standard restores are typically completed within 1-2 business days depending on data volume and validation needs - Urgent restores can be prioritised based on incident severity and support tier.

Disaster recovery (DR) & business continuity: Purview maintains documented recovery procedures for critical service components - DR testing is performed periodically as part of operational readiness - Business continuity arrangements include incident triage, alternate access procedures, and prioritised restoration of core services.

RPO/RTO (targets): Standard targets (unless contractually agreed otherwise): Recovery Point Objective (RPO) up to 24 hours and Recovery Time Objective (RTO) up to 8 hours for Purview-hosted production environments.

• Onboarding & Offboarding Support

Onboarding process: Kickoff and requirements capture (workflows, integrations, roles) - Environment setup (hosted or customer environment) - User provisioning and access setup - Configuration, integration validation, and acceptance - Training for reseller trainers/admins - Go-live support and hypercare window (as agreed).



User provisioning: User accounts can be created and managed by the Licensee through administrative functions and/or supported APIs, including role assignment and access controls (subject to configuration).

Training approach: Training is delivered to reseller trainers/admins and may include remote sessions, onboarding guides, and handover documentation. End-user training and adoption support can be provided by the reseller (standard) or by Purview under a separately scoped engagement.

Offboarding process: Account closure and access removal for users and admins - Data export and handover support (see Access to Data section) - Confirmation of service termination date and post-termination retention period - Secure deletion of customer data after the retention window, unless legally required to retain.

• Service Constraints

Maintenance windows & planned downtime: Planned maintenance will be scheduled during low-usage windows where possible and communicated in advance. Emergency maintenance may be performed to address security or stability risks.

Customisation limitations: Customisations are provided on a best-effort basis within the product's supported extension points. Source-code changes, deep platform changes, and custom forks are subject to separate commercial and technical assessment.

Dependencies & prerequisites: Supported device models/OS versions and supported browsers (see Technical Requirements Section) - Reliable network connectivity and required firewall rules/ports - Third-party services (if integrated) such as identity providers, telephony, or messaging services.

Known constraints: Service performance may vary based on device capabilities, network conditions, and customer integrations - Some functions may require internet connectivity (hosted environments) - Offline operation, if available, is limited to configured workflows and local device storage.

• Technical Requirements

Supported devices: SEVA is designed for supported Android-based smart glasses and companion Android devices as specified in the release notes and deployment guide. Device qualification may be required for new models.

Supported browsers (admin/web components, if applicable): Latest stable versions of Chrome, Edge, and Firefox. Safari support is best-effort for web portals. Older browser versions may not be supported.

Minimum system/network requirements: Internet access to Purview-hosted endpoints (HTTPS/TLS 1.2+ on port 443) - Sufficient bandwidth for media upload/download where enabled - Customer firewall/allowlisting for required domains/IPs (provided during onboarding) - For API integrations, the Licensee must provide stable endpoints and credentials as required.



Integration prerequisites: API access requires agreed authentication keys/tokens and network reachability between SEVA and the Licensee's systems. Any third-party integration prerequisites (e.g., SSO/SAML, telephony providers) must be provisioned by the Licensee.

• Outage & Maintenance Management

Incident management: Purview follows an incident lifecycle of detect/triage, contain, remediate, validate, and close. Incidents are logged and tracked through the ticketing system, with severity classification and assigned owners.

Outage communication: Customers are notified via agreed channels (e-mail and/or ticketing system). For major incidents, periodic updates are provided until resolution and a summary/root-cause report can be provided on request.

Planned maintenance communication: Planned maintenance notifications include scope, expected impact, and expected time window. Where feasible, maintenance is performed with minimal disruption.

Expected recovery times: Recovery times depend on incident severity, environment type, and root cause. Target restoration for Severity 1 incidents is prioritised in line with the support tier and DR targets in Data Backup, Restore & Disaster Recovery Section.

• Hosting Options & Locations

Hosting models: SEVA can be deployed as (a) Purview-hosted (SaaS or single-tenant managed instance) or (b) customer-hosted/on-premises. The selected model is defined in the Order Form/Statement of Work.

Cloud provider & region: For Purview-hosted deployments, hosting is provided on major cloud platforms (e.g., AWS or Azure) in the region agreed with the Licensee. The agreed country/region will be documented per deployment to meet data residency requirements.

Data residency: Customer data is stored in the agreed hosting region. Cross-region data transfer is not performed unless required for support/DR or explicitly agreed with the Licensee and permitted by applicable law.

Architecture overview (high level): A typical hosted architecture includes an application layer, API layer, and secure data storage, protected by network controls and monitoring. Separate environments (e.g., production and staging) can be provided as required.

• Access to Data (Upon Exit)

Data export: Upon termination, the Licensee may request an export of customer data generated within SEVA. Export formats may include CSV/JSON for structured records and standard file formats for any captured media (where applicable).



Timeframes: Standard export requests are typically fulfilled within 10 business days, subject to data volume and validation. Access to a terminated environment is time-bound and aligned to the contractually agreed offboarding window.

Data deletion policy: After the offboarding/export window, Purview will delete customer data from Purview-hosted environments within a standard retention period (e.g., 30-90 days), unless legally required to retain it longer. Deletion confirmation can be provided on request.

• Security

Authentication & access controls: Role-based access controls (RBAC) and least-privilege principles - Support for strong authentication methods such as password policies and optional SSO (SAML/OIDC) where configured - Administrative access is restricted to authorised personnel and logged.

Encryption: Encryption in transit using HTTPS/TLS 1.2+ - Encryption at rest for hosted data stores using industry-standard encryption mechanisms (e.g., AES-256 or cloud-managed equivalents).

Security operations: Vulnerability management including patching for critical issues and dependency updates - Secure development practices and code reviews - Logging and monitoring for security-relevant events - Periodic penetration testing (internal and/or third-party) and remediation tracking.

Compliance & privacy: Purview aligns security controls to commonly accepted standards. Specific compliance commitments (e.g., ISO 27001, GDPR, SOC 2) are provided where contractually applicable and based on deployment scope. Data processing terms and privacy obligations are governed by the applicable agreement and data protection addendum.