Service Definition: Scaleout Edge (Managed Deployment)

Scaleout Edge is a federated learning and machine learning operations orchestration platform designed to enable machine learning on distributed, sensitive data without centralizing the raw training data. The "Managed Deployment" provides a private, single-tenant control plane hosted in a Virtual Private Cloud (VPC), allowing customers to manage global edge learning and federated learning operations from a secure, centralized interface, and to securely distribute, deploy and monitor machine learning models on edge nodes.

1. PROVISIONING

Scaleout provides a private, fully-managed instance of the Software. Deployment is available via a Virtual Private Cloud (VPC) environment hosted by one of the following supported infrastructure providers:

- Google Cloud Platform (GCP)
- Microsoft Azure
- Amazon Web Services (AWS)
- Oracle Sovereign Cloud

The infrastructure provider and region are configured and operated by Scaleout in accordance with the Order Form.

Scaleout is responsible for the initial provisioning and configuration of the environment to ensure the Software is accessible to the Customer in accordance with the specifications in the Order Form.

For the avoidance of doubt, the Managed Deployment is provided exclusively as a supplier-hosted Software as a Service (SaaS) and does not involve customer-managed infrastructure

2. ONBOARDING AND OFFBOARDING SUPPORT

Onboarding. Scaleout provides a dedicated onboarding manager to assist with initial project configuration, and edge node registration. Scaleout provides a range of onboarding resources including user documentation and getting-started tutorials (html, pdf, video), online training, and onsite training. Standard onboarding typically takes 5–10 business days**.**

Offboarding. Upon termination, users can export models, metrics and metadata as described in section 10. Scaleout offers a secure, raw bulk export subject to an additional professional service fee. Following export confirmation, all customer-specific infrastructure is deprovisioned and data is purged in accordance with our sanitization policy set forth in section 8.7.

3. SERVICE LEVEL OBJECTIVES

3.1 Availability Target. Scaleout will use commercially reasonable efforts to make the Control Plane available with an Uptime Objective of 99.5% during each calendar month. This is a performance target and does not constitute a formal Service Level Agreement or a guarantee of service.

3.2 Definition of Uptime. For the purposes of this Schedule, "Uptime" is defined as the period during which the Scaleout Control Plane is accessible via the public internet. Uptime measurements apply strictly to the Control Plane and do not include the availability of individual Edge Nodes or local customer environments.

3.3 Excused Outages. The Uptime Objective does not apply to any period of downtime or inaccessibility caused by:

- Scheduled maintenance as communicated by Scaleout.
- Force Majeure events.
- Outages or failures of third-party infrastructure providers (e.g., AWS, Azure, GCP, Safespring, Oracle).
- Issues caused by the Customer's own hardware, software, or network connectivity.

4. RESILIENCY, DATA BACKUP, RESTORE, AND DISASTER RECOVERY

4.1 Resiliency. Scaleout will architect and maintain an underlying infrastructure with commercially reasonable resiliency for all data, compute, and network services. The control plane is configured with redundancy for critical services (high-availability).

4.2 Data backup and restore procedures. Scaleout leverages the automated backup and redundancy features of the underlying IaaS providers.

- Backup Frequency**:** Automated snapshots of the Control Plane metadata and model repository are taken daily.
- Retention**:** Backups are retained for 30 days.
- Restore Process**:** In the event of a primary instance failure, Scaleout initiates a restoration from the latest snapshot. The Target Recovery Time Objective (RTO) is 24 hours.

5. MONITORING AND INCIDENT RESPONSE

Scaleout will employ a system of instrumentation and observation tools to ensure that system behavior which may limit use Software is detected. Scaleout will also employ industry reasonable practices to maintain appropriate engineering personnel availability for the purposes of incident response(s).

6. SOFTWARE UPDATES AND UPGRADES

6.1 Provision of Updates. Scaleout will provide regular updates to the Control Plane software, including bug fixes, security patches, and new feature releases (collectively, "Updates").

6.2 Patch Management. Scaleout is responsible for identifying and deploying critical security patches.Critical patches are prioritized and deployed to the Managed Deployment within 10 business days of a verified stable release.

6.3 Version Support. Scaleout manages the versioning of the Control Plane. While Scaleout aims for backward compatibility with Edge Nodes, Customers may be required to update local Edge Node software to maintain connectivity with new Control Plane features.

7. MAINTENANCE AND AVAILABILITY

7.1 Scheduled Maintenance. Scaleout will occasionally perform scheduled system maintenance which requires limits to the use of part or all of the Software features, or significantly reduces features and functions during the scheduled system maintenance period. Scaleout will take a proactive approach to minimizing the need for such maintenance. Scaleout will provide at least forty-eight (48) hours' notice for any planned downtime that may impact Control Plane availability.

7.2 Emergency Maintenance. Notwithstanding the foregoing, in the event of an emergency or urgent issue which may negatively impact Scaleout's customers, Scaleout has the right to carry out unscheduled maintenance to remedy such instance(s). For the avoidance of doubt, such unscheduled maintenance shall: (i) be limited to only those issues which may negatively impact customers; and (ii) will be carried out in such a manner to provide for the least amount of disruption to customers.Scaleout will notify the Customer as soon as reasonably practicable during such events.

8. SECURITY AND COMPLIANCE

8.1 Infrastructure Security. Scaleout implements industry-standard security measures for the Managed Deployment, including multi-factor authentication for administrative access and continuous monitoring of infrastructure health.

8.2 Pass-Trough Security Warranty. The Managed Deployment is hosted on infrastructure provided by IaaS vendors (e.g., AWS, Azure, GCP, Oracle). Scaleout leverages the physical and environmental security controls of these providers, including their respective certifications for ISO/IEC 27001, SOC 2 Type II, and compliance with NCSC Cloud Security Principles. Scaleout warrants that it will configure these IaaS resources in accordance with security best practices, including encryption of data at rest and in transit using industry-standard cryptographic protocols, see Section 8.8, 8.9.

8.3 Data Isolation. The Managed Deployment is provisioned as a single-tenant environment, ensuring the Customer's models and metadata are logically isolated from other Scaleout environments:

- Separate database instances or schemas per Customer.
- Isolated object storage buckets with encryption at rest.

- Persistent Volume Claims (PVCs) scoped to customer namespace.

8.4 External Isolation (Customer-to-Customer).

- Dedicated Virtual Private Cloud (VPC) or VNet per customer with private IP addressing.
- Network-level segregation preventing cross-tenant communication.
- Separate database instances (PostgreSQL/MongoDB) per customer deployment.
- Isolated object storage buckets with customer-specific encryption keys.
- Kubernetes namespace isolation with strict Network Policies blocking inter-namespace traffic.
- Unique authentication domains (Ory Kratos/Hydra instances per tenant).
- No shared compute resources, volumes, or network paths between customers.

8.5 User-Level Isolation:

- Role-Based Access Control (RBAC) with user/admin role separation.
- OAuth2/JWT token-based authentication with user-specific permissions.
- Session isolation preventing cross-user data access.
- User-scoped API tokens with granular permissions.

8.6 Service-Level Isolation:

- Container-level isolation with separate service pods (frontend, API, controller, combiner, database).
- Kubernetes Network Policies restricting service-to-service communication to authorized paths only.
- Least-privilege service accounts for each component.
- Secrets management with service-specific credentials (no shared secrets).
- Database access controls limiting each service to required tables/collections only.
- Audit logging of all cross-service communication.

8.7 Data Residency. Scaleout ensures that all Customer Content and associated metadata reside within the geographic region specified in the Order Form.

8.8 Encryption at Rest. Scaleout configures the Managed Deployment to ensure that all Customer Content is encrypted at rest using the native encryption capabilities of the underlying IaaS provider (e.g., AWS EBS/S3 encryption, Azure Disk/Blob encryption).

- Standard: Data is encrypted using industry-standard AES-256 algorithms.
- Key Management: For this Tier, encryption keys are managed by the IaaS provider's Key Management Service (KMS) on behalf of Scaleout. These keys are protected by hardware security modules (HSMs) and are logically isolated to the Customer’s specific environment.
- Scope: This encryption applies to all persistent block storage (volumes) and object storage used by the Control Plane to store Customer models, metadata, and artifacts.

8.9 Encryption in Transit. All data moving between the Customer's Edge Nodes and the Scaleout Control Plane, as well as internal traffic within the Managed VPC, is encrypted in transit. Scaleout mandates the use of TLS 1.2 or higher (SSL) for all API communications and administrative access, ensuring that federated learning updates and metadata are protected from interception.

8.10 Data Sanitization and Logical Deletion. Upon termination of a Service or receipt of a deletion request for specific Customer Content, Scaleout shall perform a Logical Deletion of the associated data volumes via the IaaS provider's API. This action triggers the underlying IaaS provider's data sanitization protocols (designed to meet NIST 800-88 or equivalent industry standards for media sanitization), rendering the data unrecoverable within the cloud infrastructure. Scaleout confirms that all pointers to the Customer Content are removed from active system indexes during this process.

8.11 Log Retention and Auditability. Scaleout maintains centralized audit logs capturing administrative access, system events, and security-relevant actions within the Managed Deployment. Upon deprovisioning of a Customer-specific environment, Scaleout retains these system and security logs for a minimum period of twelve (12) months in Write-Once Read-Many (WORM) state. The logs are accessible to the Customer upon written request.

9. SUSPENSION OF SERVICE

Scaleout reserves the right to suspend service to the Software if: (i) Customer fails to comply with the Agreement and this Appendix, (ii) Customer exceeds set capability limits, or (iii) requests or usage deemed malicious in nature is identified to be sourced from Customer accounts, personnel, Nodes or systems. There will be a 30-day written notice before suspension, except in cases of security compromise of malicious activity.

10. DATA PORTABILITY AND EXIT PROCEDURES

10.1 Self-Service Export. For a period of thirty (30) days following termination ("Export Period"), Customer shall maintain limited access to the Control Plane solely for the purpose of exporting Customer Content. Customer may export data using the following standard methods:

- Models**:** Downloadable in original binary format via the WebUI, API and CLI.
- Metadata & Metrics**:** Exportable in JSON format via the API and CLI.

10.2 Bulk Export Services. Upon written request and subject to additional Professional Service fees, Scaleout can provide a full archive of the Customer's environment, including:

- A full export of the dedicated database.
- A complete snapshot of the Object Store.

Data can be provided via secure Cloud Storage transfer (e.g., S3/Azure Blob) or, if requested for security/size reasons, via encrypted physical storage media at the Customer's expense.

10.3 De-provisioning. After the Export Period, Scaleout will decommission the Managed Instance and permanently delete all associated Customer Content in accordance with the Data Santítization procedure outlined in 8.10.

11. SUPPORT

11.1 Support Availability and Channels

- Business Hours**:** 09:00 – 17:00 GMT, Monday through Friday, excluding public holidays.
- Channels**:** Support is accessible via designated Email, and a dedicated Slack/Discord/Teams channel.

11.2 Technical Account Manager (TAM) and after market support. Customer will be assigned a designated TAM to provide onboarding support, proactive guidance, architectural reviews, and regular health checks of the Scaleout Edge environment. The TAM will invite quarterly status update meetings to review progress, inform about updates and upgrades (Section 6), and provide input (as requested) on solution development.

11.3. Incident Priority Definitions and Response Time Table

Scaleout will categorize incidents based on the following criteria:

Priority	Definition
P1 - Critical	Total Outage: The Software is inoperable or a core function is unavailable for all users. No workaround is available.
P2 - High	Major Disruption: A significant feature is malfunctioning or performance is severely degraded. Operations are impacted but can continue with difficulty.
P3 - Normal	Minor Error: Individual features do not perform as expected, but a workaround exists or the issue affects a limited number of users.
P4 - Low	General Inquiry: Requests for information, documentation clarification, or minor feature enhancements.

11.4 Response Times

P1 Response	P2 Response	P3 Response	P4 Response
4 Hours	8 Hours	2 Business Days	5 Business Days

11.5 Technical Exclusions and Edge Node Specifics

- Control Plane vs. Edge Nodes: P1 (Critical) status is reserved exclusively for incidents where the central Control Plane is non-functional.
- Distributed Resilience: Given the distributed nature of Scaleout Edge, the failure or loss of connectivity of an individual Edge Node is classified as P3 (Normal), as the system is designed to maintain overall integrity despite localized node failures.

11.6 Out of Scope Services

The following items are considered outside the scope of standard support services:

- Solution development: Custom feature development, data science, consulting, or the integration with specific Customer workflows.
- On-site support: Technical assistance required at a Customer's physical location.

If a support request is determined to be Out of Scope, Scaleout will notify the Customer. Upon request, Scaleout can provide assistance for these items through a separate Statement of Work (SOW), subject to additional fees at Scaleout's then-current professional services rates.

11.7 Support Request Process

To receive Support Services, Customer must submit a support request through one of the following channels:

- Email: support@scaleoutsystems.com
- Private chat channel.
- Submission Requirements: Each request must include a description of the issue, the observed impact, and any relevant error logs or diagnostic data. The Response Time Target begins once Scaleout has received a complete support request containing the necessary information for triage.

11.8. Escalation Path

In the event a P1 or P2 incident is not acknowledged within the Response Time Target, Customer may initiate the following escalation path:

1. Level 1**:** Technical Account Manager (TAM) or Lead Support Engineer.
2. Level 2**:** Head of Engineering, CISO, CTO.

11.9 Service Level Remedies

If Scaleout fails to meet the P1 Response Time Target three (3) or more times in a single calendar quarter, Customer is entitled to a Service Level Review. This review will involve a joint meeting between authorized representatives of both parties to identify root causes and establish a remediation plan.

If Scaleout fails to meet the P1 Response Time Target three (3) or more times in a single calendar quarter, the Customer may be eligible for Service Credits:

- Calculation**:** Eligible Service Credits are calculated as 5% of the Monthly Subscription Fee for the month in which the third missed target occurred.
- Claim Process**:** Customer must submit a written claim for Service Credits within thirty (30) days of the end of the quarter in which the incidents occurred.
- Cap**:** Total Service Credits granted in any single month shall not exceed 20% of the Monthly Subscription Fee.
- Sole Remedy: The issuance of Service Credits shall be the Customer's sole and exclusive remedy for any failure by Scaleout to meet Response Time Targets.

11.10 Customer Obligations

In the event Customer does not reasonably comply with written specifications or instructions from Scaleout’s service engineers, regarding any support issue or request (each, a “Support Issue”), Scaleout may cease its support obligations to Customer with respect to such Support Issue upon fifteen (15) days written notice and Customer’s inability to cure such noncompliance within the notice period.