MLOPS, MODEL DEPLOYMENT AND OPERATIONALISATION

Service Definition

19 JANUARY 2026

TRIDENT INTELLIGENT SOLUTIONS

Regus Atterbury Lakes Fairbourne Drive, Atterbury, Milton Keynes, Buckinghamshire, England, MK10 9RG

Contents

Service overview

The MLOps, Model Deployment and Operationalisation service supports public sector organisations in deploying, scaling, and sustaining artificial intelligence and machine learning solutions in production environments. The service focuses on bridging the gap between model

development and operational use, ensuring models are reliable, secure, governed, and capable of delivering ongoing value.

The service covers the design and implementation of MLOps pipelines and operating processes, including model deployment, integration with existing systems and workflows, version control, monitoring and alerting, retraining and lifecycle management, and governance and compliance controls. It enables organisations to scale AI initiatives in a controlled, repeatable, and sustainable manner while maintaining transparency, performance, and regulatory compliance.

Delivery may be provided as a standalone engagement or as part of broader AI, data, or digital transformation programmes. Solutions may be deployed in customer-managed, service provider-managed, or third-party cloud environments, depending on agreed requirements and constraints.

Data backup, restore, and disaster recovery

Backups of models, training datasets (where appropriate), feature definitions, code, configurations, pipelines, and metadata are performed at predefined intervals and protected through access controls and encryption in line with ISO/IEC 27001 standards. Backup frequency and retention periods are defined per engagement, taking into account model criticality, regulatory requirements, and data sensitivity.

Disaster recovery and business continuity arrangements define roles, responsibilities, and recovery procedures for model serving infrastructure and associated pipelines. These arrangements are reviewed periodically and tested where appropriate. Where third-party platforms or cloud services are used, their resilience and continuity controls are incorporated under a shared responsibility model.

For each engagement, documentation includes:

- Assets backed up (models, code, configurations, metadata)
- Backup frequency and retention
- Storage location
- Restoration procedures
- Testing schedules
- Roles and responsibilities

Onboarding and offboarding support

Onboarding

Following contract agreement, an MLOps Lead and appropriate delivery team are assigned. An onboarding and discovery phase is conducted to understand existing models, data pipelines, target environments, governance requirements, and operational constraints.

A kick-off workshop confirms scope, objectives, success measures, delivery approach, and governance arrangements. An engagement plan or Project Initiation Document is produced and agreed, defining roles and responsibilities, dependencies, risks, and delivery milestones.

During onboarding, secure access to required systems, environments, repositories, and monitoring tools is provisioned in line with customer security policies and the principle of least privilege. Alignment is also achieved on governance, ethical AI principles, and relevant legal and regulatory requirements.

Offboarding

At the conclusion of the engagement, a formal offboarding and handover process is conducted. This includes walkthroughs of MLOps architecture, deployment pipelines, monitoring dashboards, governance processes, and operational procedures.

All artefacts—including models, code, pipelines, configurations, documentation, and runbooks—are formally handed over to the customer or successor provider. In the event of early termination, a controlled exit process and closure documentation are provided to support continuity.

Service constraints

The service is delivered during standard business hours unless otherwise agreed. The service covers models, pipelines, and environments explicitly defined in the agreed scope.

Service levels

Service levels, including deployment timelines, monitoring coverage, incident response times, and support hours, are defined and agreed at the commencement of the engagement. Service levels are tailored to model criticality, risk profile, and operational requirements.

Agreed service levels are documented in the applicable statement of work or support agreement and are reviewed periodically to ensure continued alignment with service usage and organisational needs.

Unless otherwise agreed in writing, the service and ongoing support shall be provided during standard business hours (9-5), Monday to Friday. Support outside of these hours, including 24/7 support, may be provided subject to a separately agreed arrangement.

After-sales support

Following delivery, a formal handover supports transition to business-as-usual operation. Documentation includes deployment architectures, model lifecycle processes, monitoring and alerting configurations, governance controls, and operational runbooks.

Ongoing support services may be provided where required, including model performance monitoring, drift detection, retraining support, pipeline enhancements, and compliance

reporting. These services are agreed on a case-by-case basis and delivered under retainer-based or time-and-materials arrangements.

Technical and client-side requirements

The customer is responsible for identifying relevant business owners, data science leads, technical owners, security, and governance stakeholders to support effective delivery and ongoing operation.

The service provider requires appropriate access to customer-managed or hosted environments, including cloud platforms, CI/CD tools, model registries, data pipelines, and monitoring systems. Access permissions and security controls are agreed in advance and provisioned in accordance with customer policies and the principle of least privilege.

Any additional technical prerequisites, such as data availability, integration endpoints, or identity management, are identified during onboarding to ensure timely delivery.

Outage and maintenance management

In the event of a model deployment failure or operational issue attributable to delivered MLOps components, investigation and remediation are undertaken at no additional cost, subject to agreed scope and acceptance criteria.

Issues arising from factors outside scope, such as upstream data quality problems, customer-managed infrastructure changes, third-party platform outages, or enhancement requests—may be supported under agreed maintenance arrangements.

Planned maintenance activities, including updates to pipelines, frameworks, or monitoring configurations, are coordinated with the customer to minimise disruption.

Hosting options and locations

MLOps pipelines and model serving infrastructure may be deployed within customer-managed environments, including public cloud platforms or on-premises systems, or hosted by the service provider where agreed.

Hosting providers, geographic locations, data residency requirements, resilience characteristics, and security controls are defined per engagement and documented as part of the solution design.

Data access on exit

Customers retain full ownership of all customer-provided data, trained models, code, configurations, and artefacts developed during the engagement. Upon exit, all agreed assets are made available in industry-standard formats to support continued operation or transition.

Reasonable transition support is provided for a defined period, subject to engagement terms. Any residual customer data retained by the service provider is securely deleted or anonymised in line with agreed retention schedules and applicable regulations.

Security

Security is embedded throughout the service lifecycle and aligned with recognised standards, including ISO/IEC 27001, public sector security principles, and applicable cloud shared responsibility models. This includes:

- Defined information security governance and accountability
- Risk-based security controls proportionate to data sensitivity and model risk
- Role-based access control and least-privilege principles
- Encryption of data in transit and at rest where appropriate
- Monitoring, logging, and auditability of model and pipeline activity
- Supplier and shared responsibility management
- Secure information lifecycle and exit management

Security responsibilities are shared between the service provider, the customer, and any relevant third-party providers, with control ownership defined per engagement.