
MANAGED AI AND DATA PLATFORMS

Service Definition



19 JANUARY 2026

TRIDENT INTELLIGENT SOLUTIONS

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

Contents

Service overview	1
Data backup, restore, and disaster recovery.....	2
Onboarding and offboarding support	2
Service constraints	3
Service levels.....	3
After-sales support	3
Technical and client-side requirements.....	3
Outage and maintenance management	4
Hosting options and locations	4
Data access on exit	4
Security	4

Service overview

The Managed AI and Data Platform Service provides ongoing operation, monitoring, and support of data, analytics, and AI platforms on behalf of public sector organisations. The service is



designed to ensure platforms remain reliable, secure, compliant, and performant, enabling customers to focus on using data and insights rather than managing underlying technology.

The service covers cloud-hosted and customer-managed platforms supporting data ingestion, processing, analytics, dashboards, reporting tools, AI and machine learning models, and automated workflows. Services include platform monitoring, routine maintenance, patching and updates, performance optimisation, incident management, user support, and operational assurance. The service may be provided as a standalone managed service or following delivery of platforms and solutions through separate implementation engagements.

Data backup, restore, and disaster recovery

Backups of data, models, code, configurations, and platform 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 platform and service tier, based on business, regulatory, and contractual requirements.

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

For each managed service, documentation includes:

- Assets backed up
- Backup frequency and retention
- Storage location
- Restoration procedures
- Testing schedules
- Roles and responsibilities

Onboarding and offboarding support

Onboarding

Following contract agreement, a Service Manager and dedicated support team are assigned. An onboarding and transition phase is conducted to onboard the platform into managed service, confirm scope, service tiers, and responsibilities, and establish governance and communication arrangements.

An onboarding plan is produced and agreed, covering platform overview, operational responsibilities, support processes, escalation paths, service levels, and security requirements.



Secure access to systems, environments, and tools is provisioned in line with customer policies and the principle of least privilege.

Offboarding

At service termination or transition, a formal offboarding and handover process is conducted to support continuity of service. This includes documentation of platform configuration, operational procedures, known issues, and current status.

All platform artefacts, data, code, configurations, and documentation are handed back to the customer or successor provider. Any customer data retained during service delivery is securely deleted or anonymised in line with agreed retention schedules and applicable regulations.

Service constraints

The Managed AI and Data Platform Service is delivered during standard business hours unless otherwise agreed as part of an enhanced support or on-call arrangement. The service covers platforms and components explicitly defined in the managed service scope.

Service levels

Service levels, including platform availability targets, incident response times, resolution targets, and support hours, are defined and agreed at service commencement. Service levels are tailored to platform criticality, user impact, and operational risk.

Agreed service levels are documented in the applicable managed service agreement and are reviewed periodically to ensure continued alignment with service usage and customer requirements.

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

The managed service includes ongoing operational support for in-scope platforms. Additional services, such as platform enhancements, new features, or expanded user support, may be provided under separate change requests or time-and-materials arrangements.

Regular service reviews may be conducted to assess platform performance, incident trends, capacity, security posture, and improvement opportunities.

Technical and client-side requirements

The customer is responsible for identifying service owners, technical contacts, and governance stakeholders to support effective service operation and decision-making.



The service provider requires appropriate access to platforms, environments, monitoring tools, and documentation. Access permissions are agreed in advance and provisioned in line with customer security policies and least-privilege principles.

Any dependencies on customer-managed infrastructure, data sources, or third-party services are documented as part of the shared responsibility model.

Outage and maintenance management

In the event of a service outage attributable to managed platform components, the service provider will investigate, triage, and remediate issues in line with agreed service levels and responsibilities.

Outages arising from factors outside the agreed scope, such as customer-managed infrastructure failures, upstream data issues, or third-party service outages, are managed through coordination and escalation under the shared responsibility model.

Planned maintenance, updates, and patches are scheduled in coordination with the customer to minimise disruption wherever practicable.

Hosting options and locations

Managed platforms may be hosted within customer-managed environments or hosted by the service provider for an additional fee. Hosting arrangements, cloud providers, geographic locations, data residency requirements, and resilience characteristics are agreed per engagement and documented in the managed service agreement.

Data access on exit

Customers retain full ownership of all data, models, code, configurations, and artefacts associated with the managed platforms. Upon exit, all agreed assets are made available in industry-standard formats to support continued operation or transition to another provider.

Reasonable transition support is provided for a defined period, subject to contract terms. Residual customer data held by the service provider is securely deleted or anonymised in accordance with agreed retention schedules and applicable regulations.

Security

Security is embedded throughout service delivery 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 roles
- Risk-based security controls proportionate to data sensitivity and platform criticality



- Role-based access controls and least-privilege principles
- Encryption of data in transit and at rest where appropriate
- Monitoring, logging, and auditability
- 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 in the managed service agreement.