

---

# TRAINING, CHANGE MANAGEMENT AND UPSKILLING

---

Service Definition



19 JANUARY 2026

TRIDENT INTELLIGET 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 |
| After-sales support .....                        | 3 |
| Technical and client-side requirements.....      | 3 |
| Data access on exit .....                        | 3 |
| Security .....                                   | 4 |

## Service overview

The Training, Change Management and Upskilling service supports public sector organisations in successfully adopting new digital, data, and AI capabilities by focusing on people, processes, and ways of working. The service is designed to ensure that new software, data platforms,



analytics tools, and AI systems are effectively embedded into day-to-day operations and deliver sustainable benefits.

The service provides structured training programmes, facilitated workshops, and change management support tailored to different user groups, including operational staff, managers, technical teams, and senior leaders. Activities include user enablement, organisational change management, communications and engagement planning, and the embedding of best practices to support long-term capability development and adoption.

The service may be delivered as a standalone engagement or alongside technology delivery programmes to support successful implementation and realisation of benefits.

## Data backup, restore, and disaster recovery

Where training materials, change artefacts, or limited datasets are created or used, these materials are stored securely and protected through access controls in line with ISO/IEC 27001 standards. Backup frequency and retention are defined according to the nature of the engagement and contractual requirements.

Given the people-focused nature of the service, disaster recovery arrangements primarily relate to the availability of training materials, documentation, and collaboration platforms rather than operational systems. Where third-party learning or collaboration platforms are used, their resilience and continuity controls are incorporated under a shared responsibility model.

For each engagement, documentation includes where applicable:

- Training and change artefacts backed up
- Backup frequency
- Storage location
- Restoration procedures
- Roles and responsibilities

## Onboarding and offboarding support

### Onboarding

Following contract agreement, a Change Lead and appropriate training and change management specialists are assigned to the engagement. An onboarding phase is conducted to understand organisational context, stakeholders, user groups, and adoption challenges.

A kick-off workshop is held to confirm objectives, scope, success measures, and delivery approach. A Training and Change Plan (or equivalent) is produced and agreed, defining audiences, training formats, change activities, communications approach, timeline, roles and responsibilities, and dependencies.



During onboarding, alignment is achieved on organisational policies, accessibility requirements, learning preferences, information security expectations, and any relevant public sector constraints.

### **Offboarding**

At the conclusion of the engagement, a formal offboarding and close-out session is conducted to review outcomes, adoption progress, and lessons learned. This session supports customer ownership of training materials, change artefacts, and ongoing adoption activities.

All deliverables, including training materials, user guides, recordings, change plans, communications templates, and best practice guidance, are formally handed over. In the event of early termination, a controlled exit process and closure documentation are provided.

## **Service constraints**

The service is delivered during standard business hours unless otherwise agreed. Delivery is dependent on stakeholder availability, staff participation, and timely access to required information and systems.

## **After-sales support**

Following delivery, a formal handover supports ongoing adoption and capability development. This may include access to training materials, recorded sessions, and guidance on sustaining change.

Additional support may be provided where required, such as refresher training, onboarding for new staff, coaching, or benefits realisation support. These services are agreed on a case-by-case basis and delivered under time-and-materials or retainer-based arrangements.

## **Technical and client-side requirements**

The customer is responsible for identifying appropriate sponsors, change champions, business owners, and training coordinators to support engagement, communications, and decision-making throughout the engagement.

The service provider may require access to collaboration platforms, learning management systems, or demonstration environments. Any access requirements are agreed in advance and provisioned in line with customer security policies and accessibility standards.

## **Data access on exit**

Customers retain full ownership of all training materials, change documentation, and supporting artefacts developed during the engagement. Upon exit, all agreed materials are provided in accessible, industry-standard formats.



Any customer information retained during delivery is securely deleted or anonymised in line with agreed retention schedules and applicable legal or regulatory requirements.

## Security

Security is embedded throughout service delivery and aligned with recognised information security standards, including ISO/IEC 27001, and relevant public sector security principles. This includes:

- Defined information security roles and responsibilities
- Proportionate security controls based on information sensitivity
- Role-based access controls and least-privilege principles
- Secure handling and storage of materials and information
- 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 platforms used to deliver training or change activities.