



# **SDE/TRE Airlock Design and Development**

Service Definition Document

G-Cloud 15

---

Status: Definitive

Security Commercial – In Confidence

Version no.1/0

THINKING  
BEYOND  
LIMITATIONS

# We're Kainos

Formed in 1986, we set about finding the best people to tackle the most difficult digital work. We fostered a culture where people truly care for each other and the world around them.

Our reputation for software engineering and problem-solving was quickly established, and our customers started to view us more as their colleagues

We're much bigger now, helping organisations across the globe to navigate change in more ways than ever. But some things never change, like our commitment to our people, delighting our customers, and our technical ability

Some say we're leading a quiet revolution in digital, but if you ask us, we're just doing our bit to make the world a little bit better.



3,132 amazing  
people



13 consecutive  
years of growth



40 years  
of innovation



£382m revenue  
(FY2024)



13 locations  
globally



FTSE 250 listed  
tech company



# Our core expertise

The digital revolution is already happening. We're leading from the front to help our clients **seize every digital opportunity** and be future-ready.



Cloud



Business Applications



Data and AI



Managed services



Engineering



Service and  
experience design



Workday services  
and products

- Test
- Audit
- Shield
- Deployment
- Optimisation
- Spark & Grow

# Service Description

In today's data-driven landscape for research, organisations face the critical challenge of enabling research collaboration, data sharing, and analytics while maintaining stringent security controls and regulatory compliance. Through specialist design, build and delivery services, we support clients in developing enterprise-grade Airlock capabilities for Secure Data Environments (SDEs) or Trusted Research Environments (TREs). These capabilities provide a governed gateway that supports secure, controlled, and well managed data transfer and access, helping organisations maintain consistent handling of sensitive data remains protected throughout its lifecycle.

## The Challenge

Organisations working with sensitive data - whether in healthcare, financial services, government, or research institutions - operate using Secure Data Environments that isolate confidential information from unauthorised access. However, these environments cannot exist in complete isolation. Researchers need to extract insights, analysts require datasets for processing, and partners need to collaborate on joint initiatives. Traditional methods of data transfer, such as manual review processes, email attachments, or USB drives, introduce significant security risks, lack auditability, and create operational bottlenecks that hinder productivity and innovation.

## Kainos Airlock Design and Development Services

Kainos provide specialist design and development services to support clients to transform their data transfer processes through intelligent airlock mechanisms that automate security controls while maintaining human oversight where necessary. The design of a secure

intermediary zone between the protected SDE and external destinations, can apply multiple layers of validation, scanning, and policy enforcement to every data movement request. This approach helps ensure that data leaving the secure environment has been thoroughly vetted, while data entering the environment undergoes rigorous inspection to reduce the risk of contamination or compromise.

## Configurable Capabilities

Working with your teams, we design and configure Airlock capabilities that align to your policies, tools and environments. We are able to accelerate delivery through proven reference architectures, base infrastructure and automation libraries, enabling clients to quickly implement a secure Airlock with appropriate levels of automation.

An example configuration, which we could develop with you, looks as follows:

## Example Intelligent Access Control

An Airlock capability can be designed for role-based access controls that define precisely who can request data transfers, what types of data they can access, and under what circumstances transfers are permitted. The solution could integrate with existing identity and access management platforms, leveraging organisational hierarchies, group memberships, and attribute-based policies to make granular authorisation decisions. Multi-factor authentication can be leveraged to ensure that transfer requests originate from verified users, with session management preventing unauthorised access through compromised credentials.



# Service Description

## Example Automated Security Scanning

File transfer can be designed to undergo automated security analysis as part of the Airlock capability, using customer configurable and extensible automation rules. As an example – security scanning can utilise advanced malware detection engines to scan for known threats, suspicious patterns, and zero-day exploits. Data loss prevention algorithms can be used to analyse content for sensitive information such as personally identifiable information, financial records, or proprietary intellectual property. Format validation can be enforced to ensure files conform to expected specifications and have not been manipulated to exploit parsing vulnerabilities. Finally, files that fail security checks could be automatically quarantined for investigation, supporting the prevention of potentially harmful data from reaching its destination.

## Example Policy-Driven Workflows

We can support clients to configure flexible approval workflows that match their governance requirements and risk appetite. For example, with simple transfers of pre-approved data types proceeding automatically after passing security scans, and requests involving highly sensitive information triggering multi-stage approval processes involving data stewards, security teams, and business owners. Airlock capabilities could support both synchronous and asynchronous approval patterns, with configurable timeouts, escalation procedures, and notification mechanisms to ensure timely processing in line with established security controls.

## Example Comprehensive Audit and Compliance

Every interaction can be

designed to generate detailed audit records that capture the complete context of data movements. Logs include user identity, timestamp, file metadata, security scan results and approval decisions. This audit trail provides the documentation necessary for supporting regulatory compliance, internal governance reviews, and incident investigation. The system can be built to support retention policies that align with organisational and legal requirements, while cryptographic signatures ensure log integrity and non-repudiation.

## Example Data Classification and Tagging

Our specialist services allow the incorporation of intelligent data classification capabilities to automatically identify the sensitivity level of information based on content analysis, metadata, and contextual signals. Appropriate sensitivity labelling can be applied to files that inform downstream security controls and retention policies. We can also enable users to manually tag data with project codes, research identifiers, or custom attributes that facilitate and support organisation-wide data governance and data discovery.

## Example Encryption and Data Protection

We offer security expertise and experience to ensure that data transferring through Airlock capabilities remain encrypted both in transit and at rest, using industry-standard cryptographic algorithms and key management practices. This includes use of secure transport protocols to protect data as it moves between systems, with encrypted storage to ensure that files in quarantine or staging zones cannot be accessed by unauthorised parties.

# Service Description

## Example Real-Time Monitoring and Alerting

We can support client security operations teams develop real-time visibility of data transfer activities through comprehensive monitoring dashboards. This may include tracking transfer volumes, approval latencies, security incidents, and policy violations, providing both operational metrics and security indicators. We can also enable configurable alerts to notify appropriate personnel when anomalous patterns emerge, such as unusual transfer volumes, repeated policy violations, or suspicious user behaviour, enabling rapid response to potential security incidents.

## Example Integration Ecosystem

Our Airlock design and development services offer extensive integration expertise to support clients to connect with broader security and data management infrastructure. This may include development of APIs to enable programmatic access for automation and orchestration, connectors for popular SDE platforms and cloud storage services, and collaboration tools simplify deployment and operation. Support for standard protocols and data formats to align with existing workflows and minimises disruption during implementation.

Development of these example Airlock capabilities can be accelerated with other licensed components (third party / Kainos) for additional functionality and faster delivery, subject to separate procurement.

## Benefits for Organisations

Organisations using Airlock capabilities developed with Kainos can realise

significant operational and security benefits through more consistent and well controlled data-transfer processes. Security teams gain improved visibility and confidence in the way that data movements requests are handled, supported by clearer audit trails and more consistent application of organisational policies. Researchers and analysts experience reduced friction in accessing the data they need, with automated processes helping reduce the manual effort and typically associated with manual review cycles. Compliance officers' benefit from streamlined evidence collection to support audits and regulatory inquiries. IT operations teams appreciate the reduced burden of managing ad-hoc data transfer requests through standardised, automated workflows.

## Use Cases

Kainos Airlock services supports diverse use cases across industries. Healthcare researchers can safely extract de-identified patient data for analysis within their existing compliance frameworks. Government agencies can collaborate with external partners on joint research initiatives while maintaining consistent handling of sensitive information. Pharmaceutical companies can use airlock features to support the exchange of clinical trial data with research organisations, helping protect intellectual property and research integrity. Financial institutions can share transaction datasets with regulatory authorities under controlled conditions.

# Service Description

As organisations seek to enable secure, well-governed data access, Kainos' Airlock design and development services help them establish a secure gateway that supports confident and controlled movement of data. By applying proven patterns, configurable workflows and integration expertise, we enable customers to enhance the usability, consistency and oversight of SDE/TRE data transfer operations.

## Service Terms, limitations, licensing and customer responsibilities

### 1. Nature of Service

The service provides configuration, security patterns, tooling, and accelerators for a Secure Data Environment/Airlock hosted in customer-controlled infrastructure.

### 2. Intellectual Property

The supplier retains all intellectual property in its background materials including accelerators, patterns, tooling, methods and documentation and any other pre-existing or independently developed assets used in delivering the services. Customers retain all rights in their own infrastructure and data and any customer specific materials they provide.

Kainos grants the Customer a non-exclusive licence to use the supplier background IP only as required to operate the delivered Airlock configuration within the Customer's environment. The licence does not extend to the reuse, modification, or distribution outside the agreed service scope.

### 3. Customer Responsibilities

Customers are responsible for provision of cloud tenancy and all associated cloud services, hosting costs, identity and access management, security configuration, monitoring and incident management, regulatory compliance and day-to-day operational support of the service

### 4. Security and Information Governance

The customer is responsible for applicable security controls, customer infrastructure management and compliance with information governance policies.

### 6. Dependencies and Relief

Delivery and support depend on customer-provided access, environments, and decisions. Delays caused by customer infrastructure or third parties are relief events.

# SDE/TRE Airlock Design and Development

Kainos provides specialist services to design, build and deliver customer-hosted airlock extensions for Trusted Research Environments (TRE)/Secure Data Environments (SDE) in the customer's cloud tenancy. We implement policy-driven, risk-based egress controls, semi-automated output-checking, full auditability, and integrations with existing identity, workflow, compute/ storage, aligned to Five Safes and SATRE guidance.

## Features

1. Design and implement ingress/egress configurable workflows with staged human approvals.
2. Configure automated malware, DLP and file-validation checks and quarantine handling
3. Define audit logging and reporting for all transfer activities.
4. Design encryption controls using customer key management and standards.
5. Define and configure role and project-based access control models.
6. Establish data classification and sensitivity tagging rules.
7. Translate governance policies into business rules
8. Design investigation workflows for exceptions, rejections, and controlled releases.
9. Set up monitoring, alerting, and operational thresholds for transfers.
10. Integrate with customer IAM, SIEM, and ticketing systems.

## Benefits

1. Supports reduced data leakage through consistent, workflow driven governance.
2. Provides audit-ready evidence logs to assist with regulatory compliance activities.
3. Reduces malware ingress risk through configured checks and quarantine.
4. Improves oversight using agreed reports on transfers and decisions.
5. Supports Five Safes evidence by implementing repeatable egress controls.
6. Protects sensitive outputs via role design and project isolation.
7. Reduces risk of data mishandling through monitoring rules and processes.
8. Reduces review effort by automating low risk checks safely.
9. Accelerates delivery by reusing patterns, templates, and proven approaches.
10. Supports SATRE and NHS SDE standards with controls, and evidence.





# Where we are

## The Americas

Buenos Aires  
Indianapolis  
Nova Scotia  
Toronto

## UK and Ireland

London  
Birmingham  
Belfast  
Derry  
Dublin

## Central Europe

Gdansk  
Helsinki  
Paris  
Wommelgem

# What makes us stand out



Our people



True collaboration



Innovation



Digital know-how



Common goals

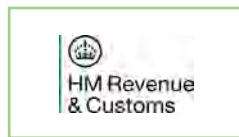


Trust



# Digital Services

We are **engineers**, specialists. We **overcome big challenges** for our clients, through delivery of **intelligent** digital services that use the best in **talent and technology**.



**55 million UK citizens**

positively impacted by  
services we've delivered



**892  
customers**



**13 locations**

And growing



**99% of customers**

rate our service as good,  
great or excellent



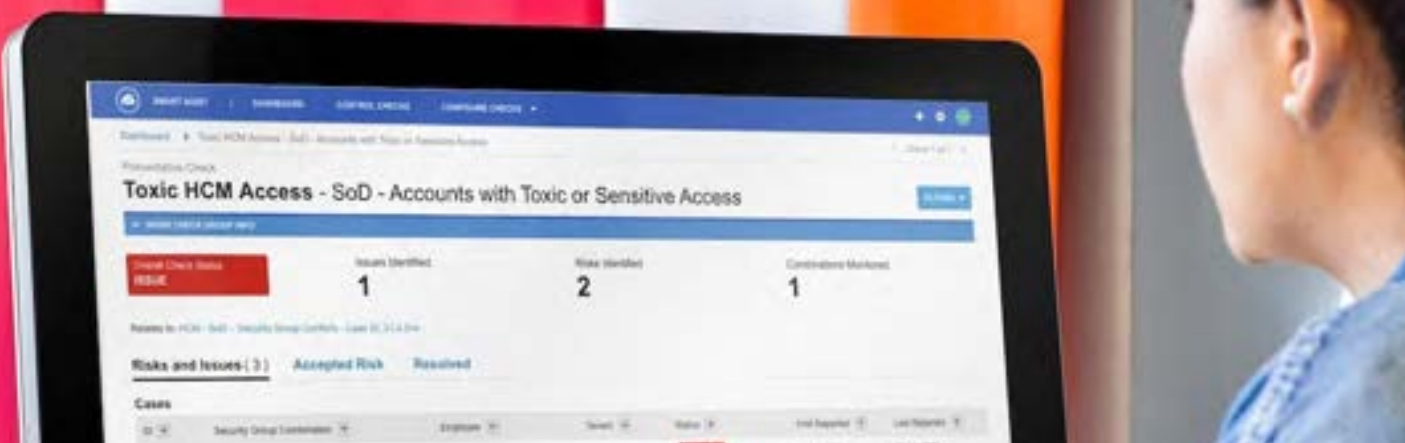
**Key partners**

Working closely with  
Microsoft and AWS to  
deliver results



**Award-winning**

90+ industry awards



# Workday

Kainos is a Workday **phase one prime status partner** in all European, North American and Asia Pacific markets. We have worked with many public and private sector customers of various sizes and scale in over **40 countries worldwide**.



## Partner Since 2011

We are the only certified Workday Services, Technology and Extend partner globally.



## Workday Services

Full range provider from pre-deployment consulting, implementation and support.



## 650+ Customers

We have deployed to over 650 customers and are a proud Workday customer also, using HCM, Financials, Recruitment, Planning and PSA to run our business.



## Workday Public Sector

We have worked with many UK Public Sector customers with their initial deployment, post-deployment support and adoption of new modules.



## Kainos Smart

Our product is deployed to 500+ customers globally saving them 1000s of testing hours.



## 900+ Consultants

Hold over 2,700+ Workday certifications covering all areas of the platform.

# 65 million

citizens positively impacted  
by services **built by Kainos**  
for the UK Government



Every driver & every car on the road  
Every piece of work to fix roads  
Every court case & every prisoner  
Every home helped with help-to-buy  
Every passport & renewal application  
Every COVID test sent out  
Every COVID test result  
Every user of the NHS App

Every voter registered  
Every company opened & closed  
Every UK civil servant trained  
Every piece of produce grown in the UK  
Every thing imported & exported to the EU  
Every benefit fraud prevented  
Every body's pension details



# Our Social Values and commitment to HM Government strategy



## Education & Capability Building

We empower people through technical and behavioral learning programs, academies, and outreach projects, fostering skills development and inspiring future technology leaders across communities and organisations.

## Social Responsibility

Tackling workforce inequality and ensuring equal access to technical and vocational education, through our Academies, Camps and Earn as you Learn schemes.

## Innovation & Future Readiness

Driving continuous improvement through technology

## Health, Wellbeing & Accessibility

We support colleagues' physical, emotional, and career wellbeing through initiatives, guidance, and inclusive design, ensuring equal access, experiences, and compliance for all users with diverse needs.

## Climate Action & Sustainability

With a comprehensive sustainability strategy underway, we will be a Carbon Net Zero company by 2030.

## Equality, Diversity & Inclusion

Maximising service experience for citizens and civil servants by delivering projects with diverse teams, underpinned by our BAME, LGBTQIA+ and female communities.



# The Code of Ethics

We are guided by our 6 ethical principles.



## Wellbeing

We protect the wellbeing of our staff, customers and communities.



## Equality

We improve access and inclusion and minimise bias.



## Transparency

Our decisions are traceable and accountable.



## Integrity

We hold ourselves and others to ethical standards.



## Environment

We act responsibly towards the Earth and its resources.



## Initiative

We take initiative to deliver social value and positive impacts.

# BCDR and Exit Plan

## **Business Continuity and Disaster Recovery (BCDR)**

A Business Continuity Plan can be provided if required. This shall set out the arrangements to be invoked in the event of an actual or perceived threat to business continuity, to ensure continued operation of the system and continuity of the services provided by Kainos pursuant to the Prime Agreement and shall include: the alternative processes, options and responsibilities that may be adopted in the event of a failure or disruption to the system and/or services provided by Kainos pursuant to the Prime Agreement; and the steps to be taken by Kainos upon resumption of the system and services provided by Kainos pursuant to the Prime Agreement in order to address any prevailing effect of the failure or disruption including a root cause analysis of the failure or disruption.

## **Exit Plan**

An Exit Plan can be provided if required to detail the steps that would be carried out to ensure smooth transition of Kainos services to a new supplier. The steps outlined in the Exit Plan will help mitigate against any disruption to the service during the transition period. It is assumed that any new supplier will themselves have a procedure they wish to follow during the transition period, and as such the steps in this Exit Plan will serve as a checklist for the new supplier to ensure all key areas of the transition have been covered. The Exit Plan will therefore be subject to refinement should it be exercised.

# Commercial Statement

## Confidentiality and copyright

© Kainos Software Limited 2026 ("Kainos")

The contents of this document are commercial and confidential in nature and the copyright of Kainos. This document must not be reproduced (in whole or in part) save in connection with the purpose for which it was issued and must not be shared with Generative AI systems without express consent.

## Trademarks

Kainos® is a registered trademark of Kainos Software Limited. All rights reserved. You may not delete or change or modify any copyright or trademark notice.

## Caveats

Kainos has used all reasonable endeavours to ensure that the contents of this document are accurate but is not responsible for any errors or omissions.

All information provided prior to execution of a contract is provided 'as is' and 'subject to contract' without warranty of any kind.

This document does not constitute an offer from Kainos. In the event that the parties elect to work together, they will only be contractually bound to each other upon signature of a contract.

## Corporate information

"Kainos" is the trading name of the Kainos group of companies, further information on which can be found here: <https://www.kainos.com/corporate-information/>.

Kainos Software Limited/ Kainos WorkSmart Limited, will be the contracting entity under this tender / for the provision of the service and may be assisted from time to time by other Kainos group companies.

## Freedom of information

Kainos considers that the following information provided in this document is exempt from disclosure under the Freedom of Information Act 2000 (FOI):

The CVs of staff qualify under the "Personal Information Exemption (s.40)" of the Freedom of Information Act and are exempt from disclosure under the Data Protection Act 1998. The Period for which this information should be confidential is the lifetime of the Data Subject.

Rate and pricing information is confidential and commercially sensitive and covered by the 'Commercial Interests' exemption (s.43) of the FOI, as the release of this information is likely to prejudice the commercial interests of Kainos and is likely to adversely affect its (and the Customer's) future negotiating position. The period that this information should be confidential for should be 5 years.