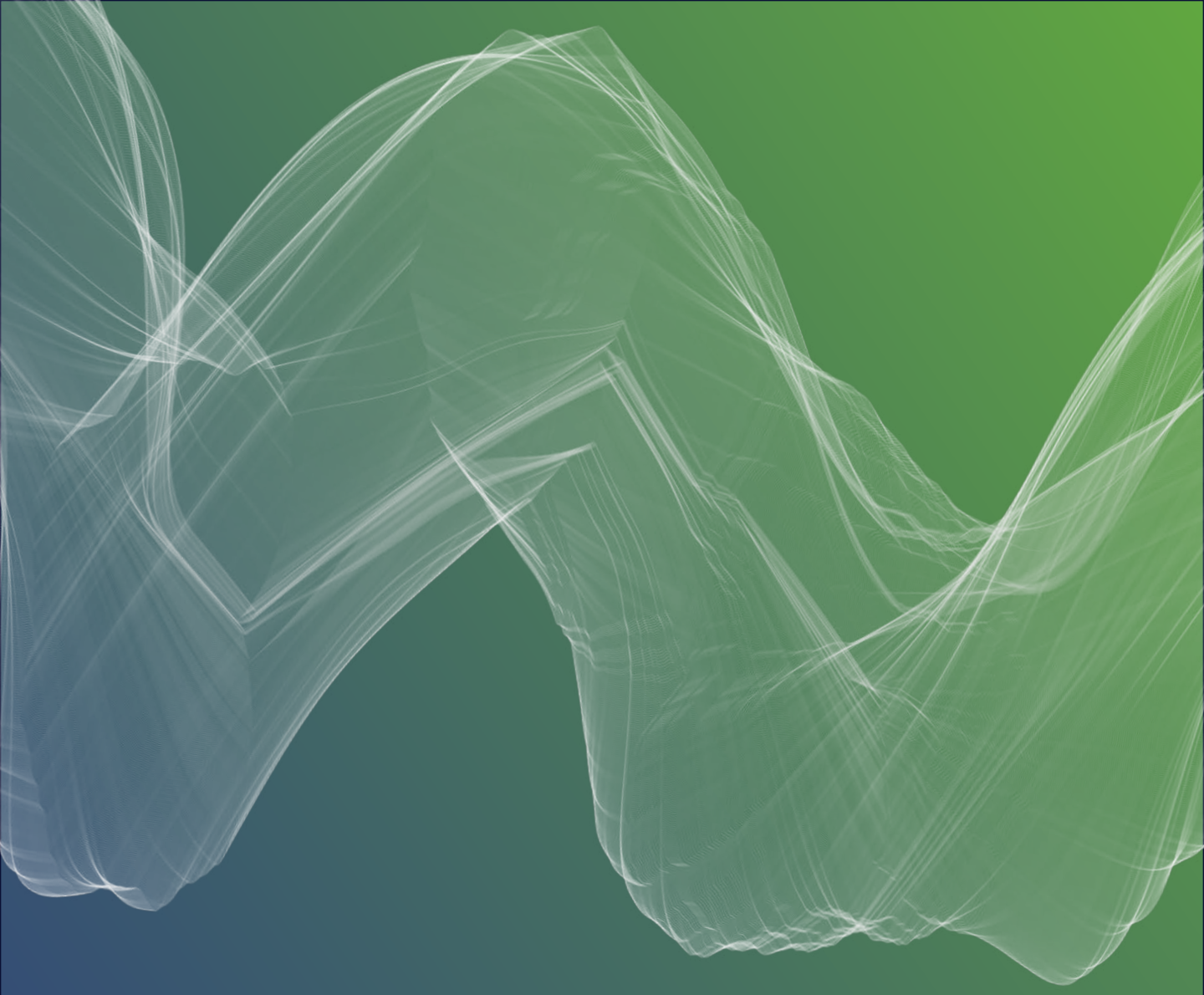


kainos®

Secure Data Environment (SDE) Design & Development

Service Definition Document

G-Cloud 15

Status: Definitive

Security Commercial – In Confidence

Version no.1/0

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

Secure Data Environment (SDE) Design & Development

Kainos provides specialist services to design, build and deliver Secure Data Environment (SDE) platforms for safely accessing sensitive data. We help organisations create governed analysis workspaces, identity and access controls and ingress/egress (Airlock/OCS) workflows, enabling researchers to collaborate on confidential datasets while ensuring strict privacy, security and regulatory compliance requirements.

Features

1. Implement security controls: encryption, segregation, logging, and audit trails.
2. Align governance to Five Safes; support DSPT CAF evidence.
3. Build standard pipelines with pseudonymisation and configurable automation.
4. Deploy and configure data analytics tooling, supporting Bring-Your-Own-License.
5. Define governed sharing workflows for multimodal data ingress/egress.
6. Design dataset management controls a nd data catalogue configuration.
7. Integrate with customer operations: monitoring, incident response, backup/restore runbooks.
8. Design scale, availability, security, and performance using cloud patterns.
9. Deliver upon buyer-approved cloud platforms using infrastructure-as-code
10. Integrate with customer IAM, SIEM, and ticketing systems

Benefits

1. Accelerate time to go-live using proven SDE/TRE design patterns.
2. Create safe and secure collaboration for all researchers.
3. Configure usage and budget controls including alerting mechanisms.
4. Mitigate vendor lock-in via customer-approved cloud agnostic portable patterns.
5. Minimise user disruption through SSO and approved BYOL support.
6. Enable faster repeat deployments through infrastructure-as-code templates.
7. Design services that scale to higher-volume workloads when required.
8. Design services supporting DSPT CAF, SATRE and ISO27001 controls.
9. Develop buyer capability through training, handover, and multidisciplinary support.

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 Secure Data Environment (SDE) platforms that enable the secure, controlled, and compliant analysis of sensitive data.

The Challenge
Organisations working with sensitive data - whether in healthcare, financial services, government, or research institutions - need Secure Data Environments (also known as Trusted Research Environments) that isolate confidential information from unauthorised access while enabling productive research and analysis. Researchers need to analyse sensitive datasets, extract insights, and collaborate on joint initiatives without compromising data security. Traditional approaches, such as providing direct database access, unrestricted computing environments, or manual oversight of every analysis step, introduce significant security risks, lack scalability, and create operational bottlenecks that hinder productivity and innovation.

Kainos SDE Design and Development Services
Kainos provide specialist design and delivery services to support clients develop SDE platforms that enforce automated controls while maintaining flexibility for legitimate research activities. Working with your teams we can configure SDE capabilities that enable the creation of isolated workspaces where researchers can access sensitive data, perform analysis using approved tools, and generate insights, all while ensuring that data cannot leave a secure perimeter without proper validation. This approach ensures that sensitive information remains protected while enabling the collaboration and innovation that drives organisational value.

We work with clients to develop a controlled, customer-hosted computing environment that enables authorised users to securely access, analyse, and collaborate on sensitive or regulated data without that data leaving the secure boundary of the customer's infrastructure.

Our services enable the replacement of traditional data-extraction and file-sharing models with isolated analytical workspaces, enforced through strong identity and access controls, network segregation, comprehensive audit logging, and continuous monitoring. This ensures that sensitive data can be used safely while maintaining compliance with applicable privacy, security, and regulatory standards.

Configurable Capabilities
Working with your teams, we design and configure SDE capabilities that align to your policies, tools and environments, building on our experience in SDE patterns and technology – using both infrastructure as code and a complex rules engine to balance security with research productivity.

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

Example Intelligent Access Control
An SDE capability can be designed to include role-based access controls that define precisely who can access which datasets, what analytical tools they can use, and under what circumstances analysis is permitted. The platform could integrate seamlessly 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 only verified users can access the environment, with session management preventing unauthorised access through compromised credentials.

Service Description

Example Secure Analysis Workspaces
Every workspace within the SDE build can be isolated and monitored through an extensible security rules that are customer configurable. As an example – workspaces could utilise pre-approved analytical tools and libraries, with continuous monitoring for suspicious activity or policy violations. Network segmentation can be used to ensure workspaces cannot communicate inappropriately, with compute resource controls prevent resource exhaustion attacks. Logging, monitored, and automat ed alerting can be designed for unusual patterns such as mass data exports, unauthorised tool usage, or access anomalies. Files leaving the environment can also be controlled by implementing comprehensive security scanning including malware detection, data loss prevention analysis, and format validation.

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 without compromising security.

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, approval decisions, and final disposition. This audit trail provides the documentation necessary for 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 Governance
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 support Data Stewards to define fine-grained permissions at the dataset, table, or column level, ensuring researchers only access the minimum necessary information, as well as defining attributes that facilitate organisati on-wide data governance, lineage tracking, and discovery.

Example Encryption and Data Protection
All data within the SDE will remain encrypted both in transit and at rest, using industry-standard cryptographic algorithms and key management practices. Network traffic is encrypted between all components, while storage encryption ensures that data-at-rest cannot be accessed by unauthorised parties. Workspace disks are encrypted and isolated, preventing cross-contamination between projects. Key rotation, certificate management, and cryptographic policy enforcement are fully automated, reducing operational burden while maintaining security posture.

Service Description

Example Real-Time Monitoring and Alerting

Customer security operations teams benefit from real-time visibility into SDE activities through comprehensive monitoring dashboards. The system design will track user sessions, data access patterns, computational workloads, egress requests, and policy violations, providing both operational metrics and security indicators. Configurable alerts notify appropriate customer personnel when anomalous patterns emerge, such as unusual data access volumes, repeated policy violations, suspicious analytical activities, or potential data exfiltration attempts, enabling rapid response to potential security incidents.

Example Integration Ecosystem

The Kainos SDE build will provide extensive integration capabilities that connect with the broader customer security and data management infrastructure. APIs can enable programmatic access for automation and orchestration, while connectors for popular data sources, analytical tools, version control systems, and collaboration platforms simplify deployment and operation. Support for standard protocols, analytical frameworks (Python, R, SQL), and data formats ensures compatibility with existing research workflows and minimises disruption during implementation. An airlock (OCS) component provides secure, controlled data ingress and egress with multi-layer validation.

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

Benefits for Organisations

- Organisations implementing the Kainos SDE custom build realise significant operational and security benefits.
- Customer security teams gain confidence that sensitive data analysis complies with organisational policies and regulatory requirements, with comprehensive audit evidence to demonstrate due diligence.
- Researchers and analysts experience a productive environment with access to necessary tools and data, with automated security processes replacing restrictive manual oversight.
- Compliance officers' benefit from streamlined evidence collection for audits and regulatory inquiries, with clear documentation of data access and usage.
- IT operations teams appreciate standardised, automated infrastructure management that reduces the burden of provisioning and securing individual research environments.

Service Description

Kainos designed SDE services enable a modern approach to balancing data accessibility with security and compliance. By automating security controls, enforcing governance policies, and providing comprehensive visibility, enabling organisations to unlock the value of their data assets while maintaining the trust of stakeholders, customers, and regulatory bodies. In an era where data breaches carry severe financial and reputational consequences, Kainos' deep expertise in delivering SDE services provides the confidence that sensitive information remains protected throughout its journey beyond the secure environment.

Service terms, limitations, licensing and customer responsibilities

1. Nature of Service
The service provides configuration, security patterns, tooling, and accelerator services for a Secure Data Environment 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 polices.

5. 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.

Where we are

The Americas

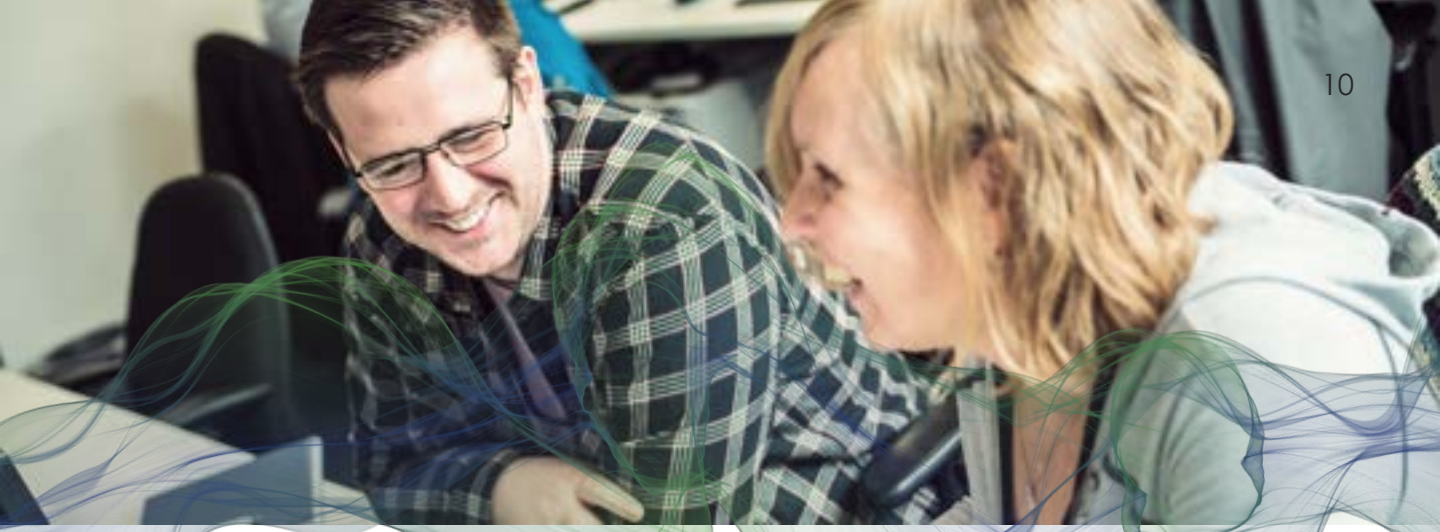
Buenos Aires
Indianapolis
Nova Scotia
Toronto

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**.

NHS
Ministry of Defence
Department for Environment Food & Rural Affairs
Department for Transport
UK Health Security Agency
Home Office
Driver & Vehicle Standards Agency
Ministry of Justice
HM Revenue & Customs
Foreign & Commonwealth Office

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

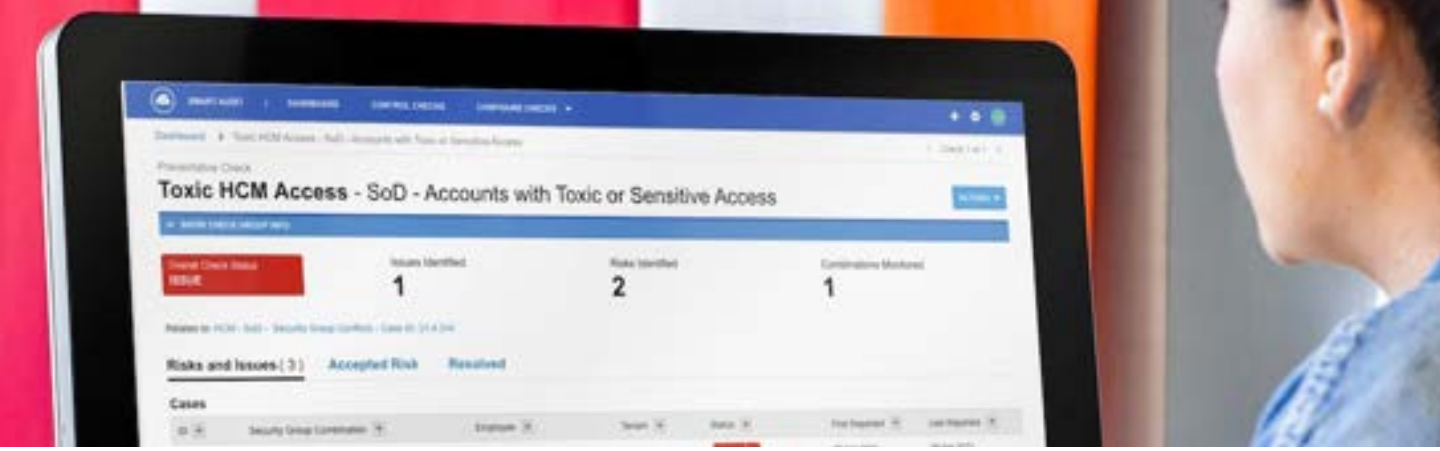
Key partners

Working closely with Microsoft and AWS to deliver results

Award-winning

90+ industry awards

kainos®



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**.

aggreko | KION GROUP | Magellan HEALTH | St. Luke's Health | The National Archives

Crown Commercial Service | Department for Education | NETFLIX | UKRI Innovate UK | Nasdaq

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

kainos®

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

Trademarks

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.