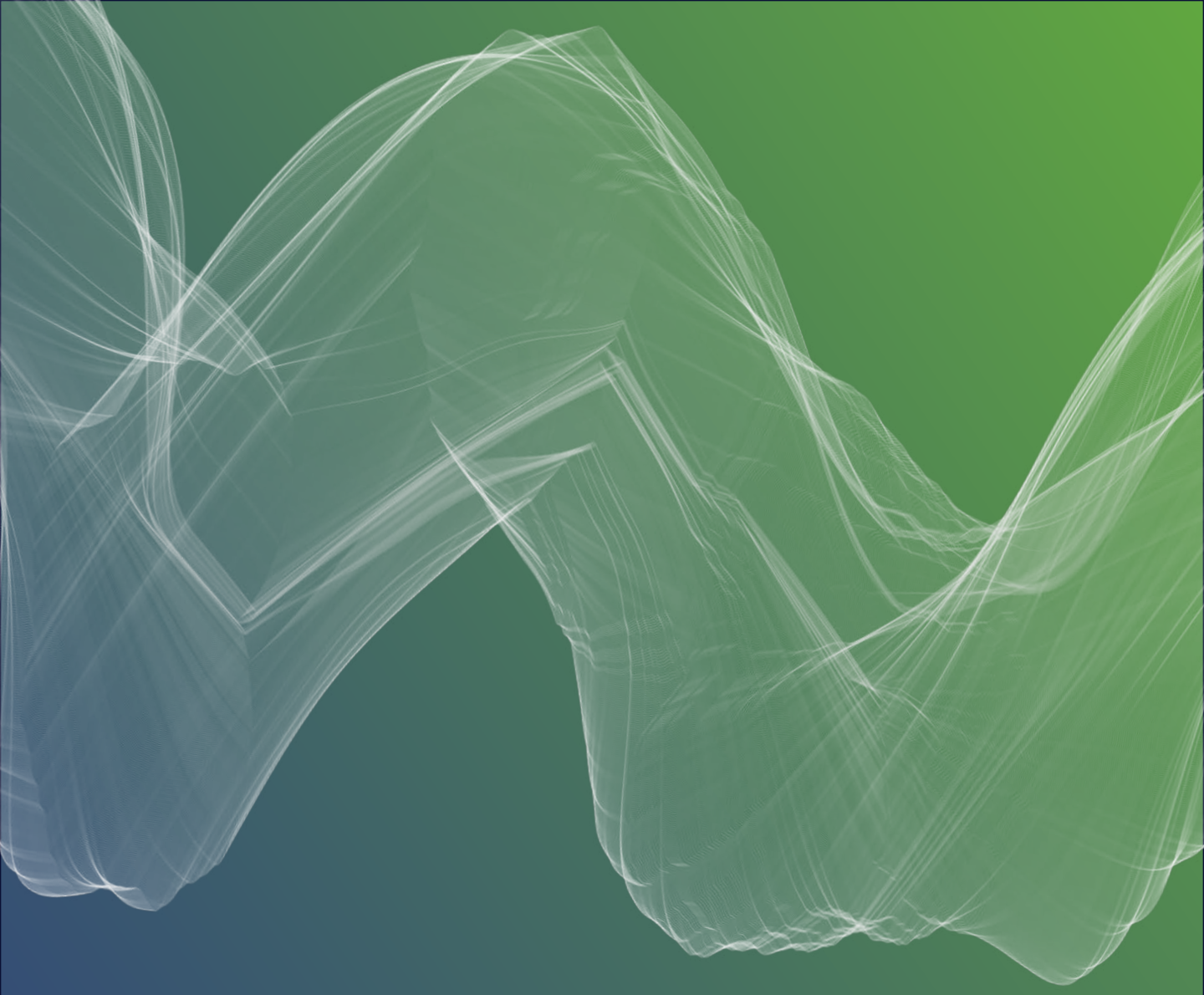


kainos®

Cyber and AI Security Protect

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

Cyber & AI Security Protect

Cyber and AI Security Protect ensures customers close identified security gaps by implementing and tuning the right controls across Microsoft Defender, Entra, Sentinel, and Purview. We harden identities, protect data, and improve detection and response, so leadership can operate confidently across modern cloud, AI, and traditional IT environments.

Features

1. **Control Implementation/Remediation,** Upd ated configurations, closure-reports, evidence of improved security.
2. **Baseline Microsoft tools ,** configured, documentation, monitoring dashboards, handover/training pack.
3. **Data Protection Enhancement,** protection configurations, DLP/encryption plans, access review logs
4. **Identity/Access Hardening,** IAM baselines, access review reports, privileged account inventories.

Benefits

1. Close high-priority security gaps quickly, with evidence of closure.
2. Turn unused Microsoft security licences into protection and visibility.
3. Reduce likelihood/impact of account compromise and lateral movement.
4. Lower risk of data leakage, insider misuse, and non-compliance
5. Achieve a defensible baseline aligned to Microsoft/UK best practice.
6. Improve detection/response times through tuned analytics and automation.
7. Protect emerging AI workloads without weakening existing IT controls.
8. Provide clear dashboards for leadership on posture, incidents, and coverage.
9. Enable internal teams with documentation, training, repeatable runbooks.
10. Give auditors/regulators clear evidence of implemented and tested controls.

Cyber & AI Security Protect

Close the gaps and strengthen your defences—fast.
Organisations today often know they have security gaps but struggle to close them at speed. Assessment reports list vulnerabilities, but internal teams lack the capacity or specialised skills to implement the necessary fixes. At the same time, the accelerating adoption of Artificial Intelligence (AI) and cloud services has expanded the attack surface, creating new risks that legacy configurations simply cannot handle.

Kainos Cyber & AI Security Protect is a Cloud Support service that translates security assessment findings into implemented controls and operational capability. We do not just advise; we roll up our sleeves and fix the problems. We harden your estate using the full power of the Microsoft security stack—**Defender, Entra, Sentinel, and Purview**—to deliver a robust, best-practice defence for both modern AI and conventional IT workloads.

Designed for CISOs, security leads, and risk officers, this service bridges the gap between "knowing" and "doing." We take the outputs from your security assessments and turn them into configured tools, defined processes, and measurable outcomes. Whether you need to lock down identity, protect sensitive government data, or operationalise threat detection, we deliver a secure, compliant baseline that allows you to innovate with confidence.

Service Components: From Assessment to Action
Our service is built around four core pillars of protection, ensuring comprehensive coverage across your technology estate.

1. Control Implementation & Remediation
Found security gaps but don't know how to fix them?
Many organisations sit on assessment reports for months because they lack the engineering bandwidth to act. We solve this paralysis.

What we do: We review your risk register or assessment findings and implement the necessary technical fixes. We update configurations, patch vulnerabilities, and deploy compensating controls where direct fixes are not possible.

The Outcome: You move from "knowing" you have a problem to "proving" it is fixed. We provide closure reports and evidence of improved security posture, satisfying auditors and internal boards.

2. Baseline Microsoft Security Tools Configuration

Overwhelmed by Microsoft security tools, or not sure they're set up right?
Public sector organisations often own powerful Microsoft E5 licences but only use a fraction of the capability. We configure your existing investment to deliver maximum value.

What we do: We establish a rigorous security baseline across **Microsoft Defender** (endpoint, server, and cloud workload protection), **Microsoft Entra** (identity), **Microsoft Sentinel** (SIEM/SOAR), and **Microsoft Purview** (data compliance). We enable critical connectors, activate analytics rules mapped to MITRE ATT&CK, and deploy standard incident response playbooks.

The Outcome: A widely adopted, government-grade foundation for monitoring, protection, and compliance at cloud scale—without buying new tools.

Cyber & AI Security Protect

3. Data Protection Enhancement
Concerned about data leaks or regulatory fines?

Data is your most valuable asset, and often your biggest risk—especially with the rise of Generative AI tools that ingest vast amounts of information.

What we do: We leverage **Microsoft Purview** to classify and protect your data throughout its lifecycle. We define Sensitivity Labels based on impact, implement Data Loss Prevention (DLP) policies to prevent unauthorised sharing (including safeguards for AI training data), and configure Insider Risk Management to detect internal threats. We also configure robust encryption at rest and in transit using Azure Key Vault.

The Outcome: Your sensitive data is secure, regardless of where it resides or moves. You reduce the risk of data exfiltration and regulatory fines, while enabling secure collaboration.

4. Identity & Access Hardening
Worried about compromised accounts or privilege misuse?
Identity is the new perimeter. If an attacker compromises an identity, they bypass your firewall. We harden your identity infrastructure to prevent unauthorised access.

What we do: We lock down your estate using **Microsoft Entra ID**. We enforce Multi-Factor Authentication (MFA) with phishing-resistant methods for critical users, implement Privileged Identity Management (PIM) to ensure just-in-time access for administrators, and configure Entra ID Governance to automate access reviews.

The Outcome: You ensure that only the right people have access to the right resources at the right time. By reducing standing privileges and enforcing granular Conditional Access policies (based on user risk, device compliance, and location), you significantly reduce the blast radius of any potential compromise.

AI-Ready Security: Protecting the New Frontier
As AI adoption grows, security cannot be an afterthought. We ensure your Microsoft security estate protects AI workloads alongside conventional IT, without creating new silos.

Secure by Design: We configure specific controls for AI services, such as monitoring access to Azure OpenAI instances and protecting the integrity of AI training datasets.

Integrated Defence: We treat AI as part of your wider estate, ensuring that alerts from AI systems flow into Microsoft Sentinel alongside your standard IT security logs, giving you a single, unified view of risk.

Cyber & AI Security Protect[7]

Delivery Methodology
We employ a phased, low-risk delivery methodology designed to demonstrate value quickly while ensuring operational stability.

- **Phase 1: Discovery & Design.** We review your existing security posture (leveraging outputs from prior assessments where available) and design the target state configuration for Defender, Entra, Sentinel, and Purview.
- **Phase 2: Build & Configure.** We deploy the agreed configurations, typically starting in a non-production or pilot environment. This includes setting up connectors, configuring policies, and building custom analytics rules.
- **Phase 3: Test & Validate.** We rigorously test the implemented controls to ensure they function as intended and do not disrupt business operations. This involves User Acceptance Testing (UAT) for identity flows and simulation testing for detection logic.
- **Phase 4: Deploy & Tune.** We roll out the configurations to production in controlled waves to manage change impact. We then perform a critical period of "tuning"—especially for Sentinel and Defender—to minimise false positives and optimise detection efficacy.
- **Phase 5: Handover & Enablement.** We provide comprehensive "as-built" documentation and runbooks. Crucially, we deliver knowledge transfer sessions to your security operations team, ensuring they are confident in operating and maintaining the new capabilities.

Key Outcomes
By the end of the engagement, you will receive:

- **Configured Security Environment:** Fully operational instances of Microsoft Defender, Entra, Sentinel, and Purview, tuned to best practices.
- **Configuration Documentation:** Detailed "as-built" records of all settings, policies, and rules implemented, ensuring you have a clear audit trail.
- **Bespoke Control Register:** A specific record of all custom controls designed to address your unique risks.
- **Security Dashboards:** Custom workbooks in Sentinel and dashboards in Defender, providing real-time leadership visibility of security posture and compliance.
- **Operational Runbooks:** Step-by-step guides for common security tasks (e.g., responding to a specific alert type, onboarding a new privileged user).

Training Materials: Slide decks and recordings from knowledge transfer sessions to support onboarded staff.

Support and Sustainability
Kainos designs PROTECT engagements to build sustainable capability within your organisation. We do not just "switch on" tools and leave; we ensure your team understands *why* they are configured that way and *how* to manage them long-term. Our handover process includes detailed training on interpreting alerts, managing policies, and performing routine maintenance.

Why Choose Kainos PROTECT?
Microsoft Partner of the Year: We are a leading Microsoft partner with deep, verified expertise across the entire security stack. Our solutions are built on proven, field-tested configurations that we have deployed across central government and healthcare.
Public Sector Pedigree: We understand the unique challenges and regulatory requirements of the UK public sector. Our controls are designed to align with government standards (such as Secure by Design) and best practices.
Integrated Approach: We view security as an enabler, not a blocker. Our PROTECT service is integrated with our wider digital transformation and AI offerings, ensuring security is baked in from the start—not bolted on at the end.
Focus on Outcomes: We do not just deploy technology; we solve business problems. Our primary focus is on closing gaps, reducing risk, and enabling you to operate with confidence.

Where we are

The Americas

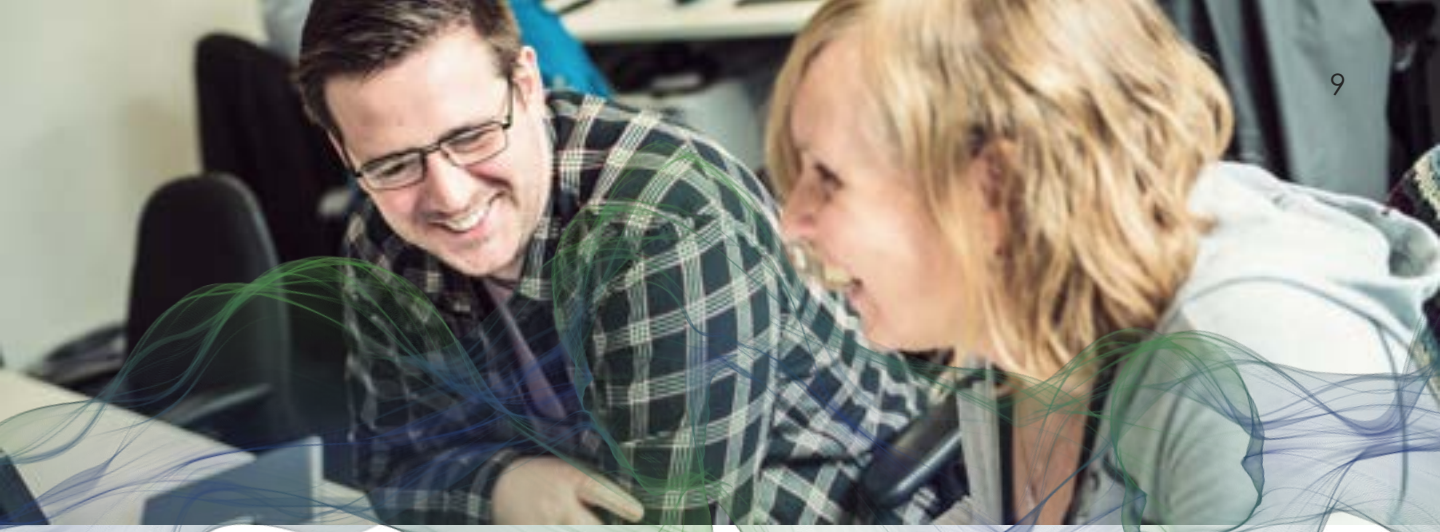
Buenos Aires
Indianapolis
Nova Scotia
Toronto

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

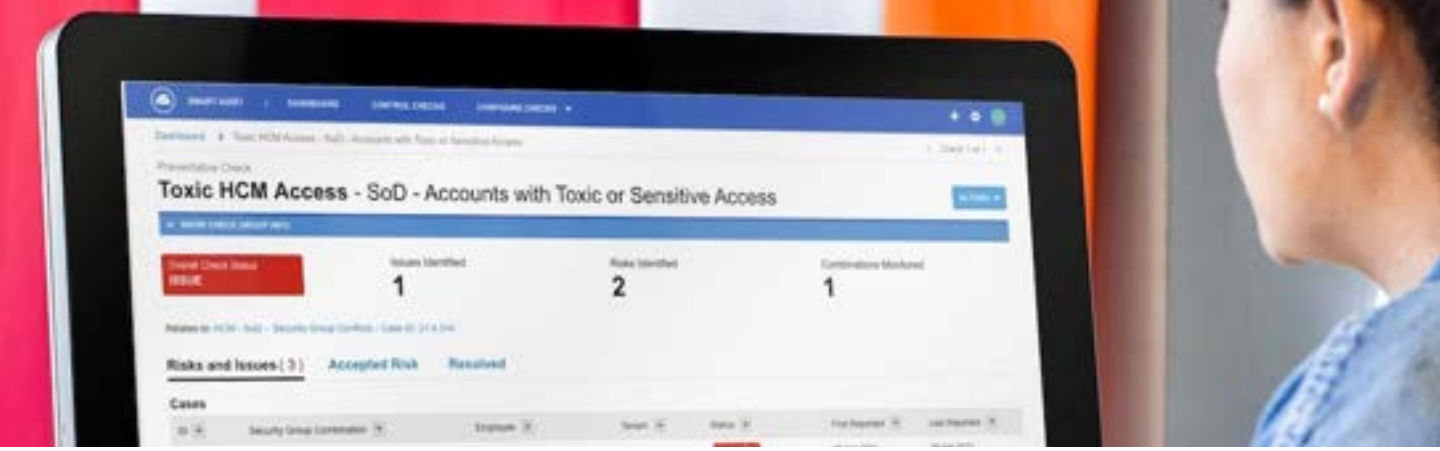
Key partners

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.