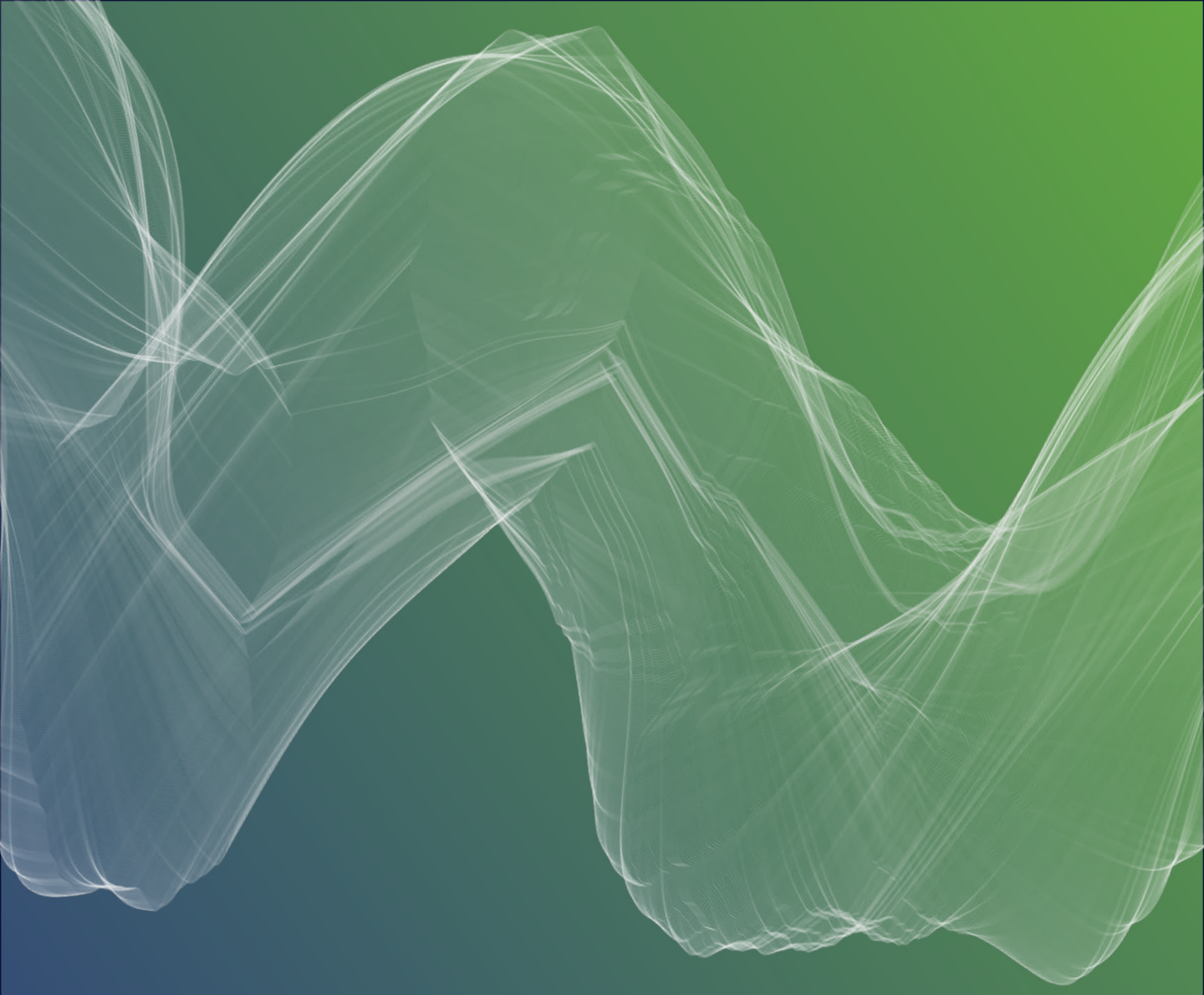


kainos®

Cyber and AI Security Governance

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 Governance

Our Cyber and AI Security Governance service ensures customers establish clear accountability, tailored risk methodologies, and practical control frameworks across IT and AI environments. We map controls to standards like NIST and ISO, enabling leadership to simplify policy management, spot hidden risks, and maintain robust strategic oversight, so they can govern with confidence.

Features

1. **Security Governance Framework,** governance diagrams, role/responsibility charts, reporting templates.
2. **Risk Management Framework, r**isk process documentation, risk-appetite statements, scoring tools.
3. **Controls Framework, c**ustom control catalogue, mapped objectives, ownership matrix.
4. **Policy & Standards Framework,** policy templates, authoring guides, review checklists.

Benefits

1. Establish **clarity and confidence** in security leadership
2. Reduce risk with **structured governance and control frameworks**
3. Ensure compliance with **industry and regulatory standards**
4. Improve decision-making through **transparent reporting and accountability**
5. Enable faster response with **defined escalation processes**
6. Build a strong foundation for **AI and cyber resilience**
7. Simplify compliance with **practical, user-friendly policies**
8. Enhance organisational trust and **board-level visibility**
9. Support long-term security strategy and **continuous improvement**
10. Align security with **business objectives and risk appetite**

Cyber & AI Security Governance

Governance that enables, not strangles.
Organisations today face a dual governance crisis. IT cybersecurity governance frameworks—designed for a slower era—often exist on paper but remain unenforced in practice. Simultaneously, the rapid adoption of Artificial Intelligence (AI) has introduced a new frontier of risk that most existing structures are ill-equipped to handle. Policies gather dust, AI adoption outpaces approval, and critical decisions are delayed by bureaucracy.
The result is a dangerous gap: teams lack clarity, leadership lacks visibility, and the organisation faces mounting operational friction and unmanaged risk exposure.

Kainos Cyber & AI Security Governance is a comprehensive framework and operating model design service. We establish exactly how your organisation should govern, manage, and measure cybersecurity risks at board, management, and operational levels. Rather than imposing generic templates, we design tailored governance structures, practical policies, risk management processes, and control standards mapped specifically to your business context, regulatory landscape, and organisational maturity.
Our approach is grounded in the newly published **NIST Cybersecurity Framework 2.0**, which elevates **GOVERN** as a core function equal to Identify, Protect, Detect, Respond, and Recover. We align your governance with **ETSI TS 104 223** (the European baseline for securing AI), **ISO 27001**, the **NCSC Cyber Assessment Framework (CAF)**, and **EU AI Act** compliance requirements. The result is a unified operating model that satisfies multiple regulatory mandates simultaneously, transforming governance from a checkbox exercise into a strategic enabler.

Why Governance Matters Now
The landscape has shifted. Governance is no longer just about compliance; it is about survival and speed.

1. Governance is now foundational to security.
The NIST CSF 2.0 'GOVERN' function recognises what leading organisations already know: all other security activities fail without clear governance. If you cannot decide who owns a risk, you cannot mitigate it. Yet, many organisations still treat governance as an administrative burden rather than the central nervous system of their security posture.
2.Weaponised AI has accelerated the threat landscape.
AI-driven attacks move faster than manual governance processes can accommodate. Thirty-day patch cycles and annual policy reviews create vulnerability windows that adversaries can exploit in minutes. Classic governance structures, designed for a static threat environment, are becoming obsolete.
3. AI adoption is outpacing control.
Business units are eager to deploy generative AI, machine learning models, and autonomous agents to drive innovation. However, without clear AI governance—such as risk assessment gates, model validation, and supply-chain vetting—organisations face unmanaged, potentially catastrophic risks including model drift, data poisoning, adversarial manipulation, and prompt injection.
4. Board-level accountability is non-negotiable.
Regulators, investors, and audit functions now demand board-level oversight of combined IT and AI cyber risks, fully integrated with Enterprise Risk Management platforms. Governance that remains hidden in technical GRC systems fails this test. Leadership needs intelligible dashboards to make informed risk acceptance decisions.
5. Regulation is tightening whilst innovation accelerates.
The EU AI Act, ETSI standards, and UK DSIT guidance demand explicit governance for AI systems. Organisations cannot afford to slow innovation to navigate this complexity. The answer is not "governance *or* speed"—it is "governance that *enables* speed."

Cyber & AI Security Governance

The Governance Challenge

Most organisations we encounter struggle with three core problems:

Problem 1: Unenforced Cyber security Governance.

Cybersecurity policies regarding access control, incident response, and vendor management exist, but they are not enforced. Teams ignore them, compliance officers cannot audit them, and leadership is unaware of the gaps until a breach occurs.

Problem 2: Immature AI Security Governance.

AI security governance is often nascent or entirely absent. There is no approved list of AI tools, no risk assessment for machine learning pipelines, and no vetting for third-party models. Risks accumulate silently, and by the time they surface, the reputational and operational damage is done.

Problem 3: Governance Friction.

When governance does exist, it often stifles innovation. Design Authority approval cycles take weeks, policy updates stall in committee, and research teams view security as a blocker. This friction leads to "shadow IT" and "shadow AI," where teams bypass governance entirely to get work done.

How We Solve It: A Unified Framework

We help you set the rules, define what "good" looks like, and ensure your leadership is always in the driving seat—across both AI and conventional cyber security.
Establish clear security ownership and accountability at every level.
Define risk management processes that fit your business and regulatory landscape.
Set out exactly which controls and policies you need—no more guesswork.
Make security policies practical, understandable, and actionable.

Let us give your organisation the clarity and confidence to lead on security, not just react to threats.

Security Governance Framework

Struggling with unclear security ownership or board-level accountability?
We help you establish who's responsible for security, how decisions get made, and how to keep your leadership informed—so you never face confusion in a crisis.

Service: Provides a tailored, board-level framework for how the organisation should govern AI and cyber security—covering leadership, roles, policies, and accountability.
Outputs: Governance structure diagrams, role/RACI charts, policy hierarchy, board reporting templates.

Risk Management Framework

Worried you're missing hidden risks, or unsure how to prioritise them?
We define a risk process tailored to your business, so you can spot, score, and escalate both AI and cyber risks before they become incidents.
Service: Establishes how the customer should identify, assess, and manage AI and cyber risks, including risk appetite, scoring, and escalation.
Outputs: Risk management process documentation, risk appetite statement, risk scoring matrix, escalation flowcharts.

Security Control Framework

Uncertain what "good" security looks like for your organisation?
We set out exactly which controls you should have in place for AI and IT, mapped to NIST, ISO, and regulatory standards, so you know where you stand and what's missing.
Service: Defines what "good" security controls look like for both AI and conventional IT, mapped to NIST, regulatory, and sector standards.
Outputs: Customised control catalogue, control objectives, mapping to NIST/ISO/AI Act, control ownership matrix.

Cyber & AI Security Governance

Policy & Standards Framework
Policies gathering dust, or too complex to follow?
We give you practical templates and guidance to create policies people actually understand and use, making compliance achievable, not a checkbox exercise.
Service: Provides templates and guidance for writing effective security policies and standards, ensuring clarity, enforceability, and alignment with business objectives.
Outputs: Policy/standards templates, authoring guide, review checklist, policy lifecycle workflow.

Why Kainos
Kainos brings a unique blend of government-grade security heritage and cutting-edge AI expertise.

- **Government-Grade Experience:** We have delivered secure critical national infrastructure for the **NHS App** (30M+ users, zero critical incidents) and a Securing Digital Justice platform for **HM Courts & Tribunals Service** (4,900% increase in deployment frequency; lead times improved 3,000%, £1.2m operational savings).
- **AI Governance Leadership:** We co-authored the **DSIT/NCSC AI Cybersecurity Code of Practice** (now aligned to ETSI TS 104 223) and are active contributors to the **OWASP Top 10 for Agentic Applications**.
- **Practical Delivery:** We do not just write theoretical strategy documents; we embed executable governance into development workflows that engineering teams can follow.
- **Multi-Framework Expertise:** Our teams are deeply experienced in mapping complex requirements across NIST, ISO, CAF, and emerging AI regulations into a single, cohesive operating model.

Service Deliverables

- **Security Governance Framework:** Documenting roles, structure, decision rights, and escalation paths.
- **RACI Matrix & Committee Charters:** Defining precise responsibilities for all governance bodies.
- **AI Governance Framework:** Including risk taxonomy, acceptable use, and model governance standards.
- **Policy & Standards Templates:** A complete pack of strategic, operational, and technical policies.
- **Unified Control Catalogue:** Mapped to NIST, ISO, CAF, GovAssure, EU AI Act, and ETSI.
- **Design Authority Toolkit:** Including "Approval Compass," risk scorecards, and evidence templates.
- **Risk Appetite Statement:** With a tailored risk scoring methodology.
- **Board Reporting Dashboards:** Including KPI definitions and visualisation templates.
- **Governance Operating Manual:** Runbooks for maintaining the governance lifecycle.
- **Maturity Assessment:** A baseline assessment with an 18–24 month transformation roadmap

Where we are

The Americas

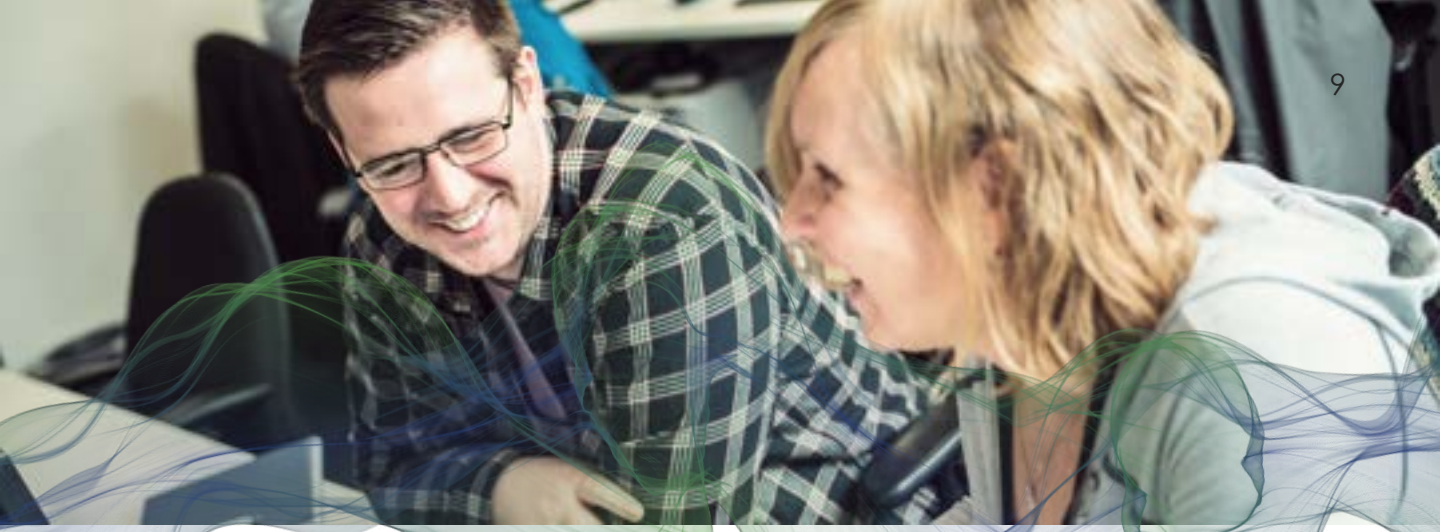
Buenos Aires
Indianapolis
Nova Scotia
Toronto

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

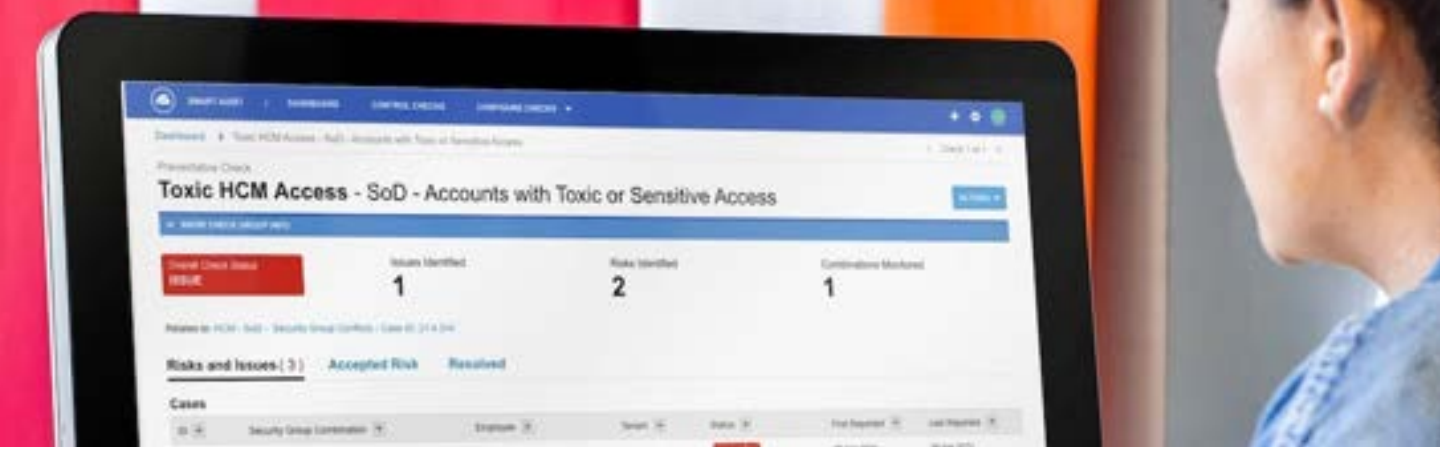
Key partners

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.