Technical and Organisational Measures

Kinetic

Effective Date: 17/02/25
CLASSIFICATION: PUBLIC

Version	Date	Description	Author	Approved By
1.0	17/02/2026	Initial Implementation	Ryan Davies	Mark Tucker

Aligned to:

- UK GDPR Articles 5, 25, 28, 32, 33, 34, 35
- Data Protection Act 2018
- ISO/IEC 27001:2022 (Annex A controls)

1. CONFIDENTIALITY

Legal Basis:

- UK GDPR Article 5(1)(f) – Integrity and Confidentiality Principle
- UK GDPR Article 32(1)(a) and (b) – Security of Processing
- UK GDPR Article 28(3)(c) – Processor Security Obligations
- Data Protection Act 2018 (as applicable)
- ISO/IEC 27001 Annex A.5, A.7, A.8, A.9, A.10, A.11, A.13

Objective:
To prevent unauthorised access to, or disclosure of, Personal Data.

1.1 Hosting Environment & Infrastructure Security

(ISO 27001 Annex A.5, A.8, A.12, A.13)

Certain services are hosted within the Microsoft Azure cloud environment. Where applicable, Kinetic Software adopts Microsoft Azure's certified security controls covering:

- Physical security
- Environmental safeguards
- Infrastructure resilience
- Logical isolation
- Secure data centre operations

Microsoft Azure maintains certifications including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and SOC 2.

Kinetic Software implements additional application-layer, identity, and monitoring controls to supplement Azure's baseline protections.

This supports compliance with UK GDPR Article 32(1)(a) and DPA 2018 security obligations.

1.2 Physical Access Control

(ISO 27001 Annex A.7, A.11)

Access to facilities is restricted to authorised Kinetic Software personnel only.
Controls include:

- Magnetic or chip-based access cards
- Physical key controls
- Alarm systems
- CCTV monitoring
- Microsoft Azure-managed physical security for hosted environments

These measures prevent unauthorised physical access to systems processing Personal Data.

1.3 Electronic Access Control

(ISO 27001 Annex A.9 – Access Control)

Unauthorised access to Kinetic Software systems is prevented through:

- Network firewalls
- Secure password policies and enforced complexity
- Encryption of storage media
- Centralised Identity and Access Management (IAM)

Multi-Factor Authentication (MFA) is enforced via a company-wide Okta identity platform, ensuring strong authentication controls for administrative and internal access.

These controls satisfy UK GDPR Article 32(1)(b) requirements for ensuring ongoing confidentiality.

1.4 Internal Access Control (Role-Based Access)

(ISO 27001 Annex A.9.1–A.9.4)

Access to Personal Data is restricted on a need-to-know basis using Role-Based Access Control (RBAC).

Controls include:

- Documented access control procedures
- Segregation of duties
- Mandatory MFA via Okta
- Logging of authentication and access events
- Periodic review of user permissions

These measures prevent unauthorised reading, copying, alteration, or deletion of Personal Data in accordance with UK GDPR Article 32(1)(b).

1.5 Isolation & Segregation of Data

(ISO 27001 Annex A.8, A.13)

Personal Data is logically or fully system-separated depending on product architecture and risk assessment.

Isolation measures include:

- Logical customer tenancy separation
- Environment-based access controls (production vs non-production)
- Network segmentation where applicable
- System-level separation depending on product design

This supports UK GDPR Article 25 (Data Protection by Design and Default) and Article 32 security obligations.

1.6 Pseudonymisation & Anonymisation

Legal Basis:

- UK GDPR Article 25 – Data Protection by Design and Default
- UK GDPR Article 32(1)(a) – Pseudonymisation and Encryption
- Data Protection Act 2018 – Security of Processing

(ISO 27001 Annex A.10 – Cryptography)

Where appropriate and proportionate to risk, Kinetic Software implements pseudonymisation and anonymisation techniques.

These are particularly applied where:

- PCI-certified environments require enhanced controls
- Data minimisation is necessary
- Risk assessments identify re-identification exposure

Controls may include:

- Tokenisation
- Masking of sensitive data
- Partial redaction
- Secure separation of identifying attributes
- Field-level encryption

These measures reduce identifiability and mitigate data breach impact risk.

2. INTEGRITY

Legal Basis:

- UK GDPR Article 5(1)(f) – Integrity and Confidentiality Principle
- UK GDPR Article 32(1)(b) – Security of Processing
- Data Protection Act 2018 – Security Requirements
- ISO/IEC 27001 Annex A.12, A.13

Objective:
To ensure the accuracy, completeness, and reliability of Personal Data.

2.1 Data Transfer Control

(ISO 27001 Annex A.13 – Communications Security)

All Personal Data transmitted electronically is encrypted in transit.
Controls include:

- TLS 1.2 or higher enforced as minimum standard
- HTTPS certificate-based communication
- Encrypted APIs
- Secure file transfer protocols

These measures prevent unauthorised reading, copying, modification, or deletion during transmission and support UK GDPR Article 32(1)(a).

2.2 Data Entry & Change Control

(ISO 27001 Annex A.12.1, A.12.4)

Kinetic Software maintains traceability and accountability for system and data changes.
Controls include:

- Activity logging of user and administrative actions
- Formal change management procedures
- Documented approval workflows
- Version control where applicable

These controls enable verification of when, how, and by whom Personal Data is entered, modified, or deleted, supporting accountability under UK GDPR Article 5(2).

2.3 Data Integrity Monitoring

(ISO 27001 Annex A.12 – Operations Security)

Technical measures are implemented by Kinetic Software to detect unauthorised system or file changes.
Controls include:

- Endpoint Detection and Response (EDR) via CrowdStrike
- File Integrity Monitoring (FIM) through CrowdStrike on hosted instances
- Continuous monitoring of system events
- Patch management and vulnerability remediation processes

These controls maintain data accuracy and detect unauthorised alterations in line with UK GDPR Article 32(1)(b).

3. AVAILABILITY AND RESILIENCE

Legal Basis:

- UK GDPR Article 5(1)(f) – Integrity and Confidentiality Principle
- UK GDPR Article 32(1)(b) – Ability to Ensure Ongoing Confidentiality, Integrity, Availability and Resilience
- UK GDPR Article 32(1)(c) – Ability to Restore Availability and Access in a Timely Manner
- UK GDPR Article 32(1)(d) – Regular Testing and Evaluation
- Data Protection Act 2018 – Security of Processing Requirements
- ISO/IEC 27001:2022 Annex A.5, A.7, A.8

Objective:
To ensure that Personal Data and supporting systems remain accessible, resilient, and recoverable in the event of physical or technical incidents, and that processing services maintain continuity in accordance with regulatory and contractual obligations.

3.1 Availability Control

(ISO/IEC 27001 Annex A.8.13 – Information Backup; A.7.11 – Supporting Utilities; A.8.7 – Protection Against Malware; A.5.29 – Information Security During Disruption)

Technical and organisational measures are implemented to ensure that Personal Data and supporting systems remain available and protected against disruption.

Controls include:

- Backup strategy (online and offline; on-site and off-site)
- Defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
- Uninterruptible Power Supply (UPS) for critical systems
- Anti-malware and virus protection controls
- Documented reporting procedures for system events
- Business contingency planning

These controls ensure ongoing availability and resilience of processing systems in accordance with UK GDPR Article 32(1)(b) and Article 32(1)(c).

3.2 Disaster Recovery & Timely Restoration

(ISO/IEC 27001 Annex A.5.30 – ICT Readiness for Business Continuity; A.8.14 – Redundancy of Information Processing Facilities)

Measures are implemented to ensure the timely restoration of access to Personal Data in the event of a physical or technical incident.

Controls include:

- Documented disaster recovery plans
- Defined and tested recovery procedures
- High availability system design
- Load balancing across infrastructure components
- Failover mechanisms to alternate systems or environments
- Regular testing of recovery capabilities

These controls support timely recovery and restoration of processing capabilities in line with UK GDPR Article 32(1)(c).

3.3 Architectural Resilience & System Hardening

(ISO/IEC 27001 Annex A.8.8 – Management of Technical Vulnerabilities; A.8.9 – Configuration Management; A.8.14 – Redundancy)

Architectural and operational safeguards are implemented to reduce the likelihood of service interruption or data compromise.

Controls include:

- High availability architecture design
- Load balancing across production environments
- Controlled software update and upgrade processes
- Formal patch management procedures
- Vulnerability identification and remediation processes

These measures maintain system resilience and operational integrity in accordance with UK GDPR Article 32(1)(b) and Article 32(1)(d).

4. EFFECTIVENESS – REGULAR TESTING, ASSESSMENT AND EVALUATION

Legal Basis:

- UK GDPR Article 5(1)(f) – Integrity and Confidentiality Principle
- UK GDPR Article 5(2) – Accountability Principle
- UK GDPR Article 25 – Data Protection by Design and Default
- UK GDPR Article 28 – Processor and Sub-Processor Obligations
- UK GDPR Article 32(1)(d) – Regular Testing, Assessment and Evaluation of Technical and Organisational Measures
- UK GDPR Articles 33 and 34 – Personal Data Breach Notification
- Data Protection Act 2018 – Security of Processing Requirements
- ISO/IEC 27001:2022 Annex A.5 and A.6 (Organisational Controls)

Objective:
To ensure that technical and organisational security measures are regularly tested, assessed, and evaluated for effectiveness, and that governance, accountability, and incident response processes remain robust, documented, and capable of supporting compliance with applicable data protection legislation.

4.1 Security Awareness & Training

(ISO/IEC 27001 Annex A.6.3 – Information Security Awareness, Education and Training)

Organisational measures are implemented to ensure personnel understand their data protection and information security responsibilities.

Controls include:

- Mandatory user awareness training
- Periodic refresher training (at least yearly as mandatory)
- Security and privacy policy acknowledgement
- Role-specific security training where appropriate

These measures support the integrity and confidentiality principle under UK GDPR Article 5(1)(f) and organisational security obligations under Article 32(4).

4.2 Data Protection Impact Assessments & Risk Management

(ISO/IEC 27001 Annex A.5.7 – Threat Intelligence; A.5.9 – Inventory of Information; A.5.36 – Compliance with Policies and Standards)

Risk-based controls are implemented to assess and mitigate privacy and information security risks.

Controls include:

- Continued use of Data Protection Impact Assessments (DPIAs)
- General information security risk assessments
- Periodic review of processing activities
- Risk treatment planning and tracking

These controls support compliance with UK GDPR Article 35 (DPIAs), Article 25 (Data Protection by Design and Default), and Article 32.

4.3 Incident Response Management
(ISO/IEC 27001 Annex A.5.24–A.5.27 – Information Security Incident Management)

A structured incident response framework is maintained to detect, manage, and remediate security incidents involving Personal Data.

Controls include:

- Corporate incident handling procedures
- Defined incident classification and escalation processes
- Documented breach assessment procedures
- Internal reporting channels for security events
- Post-incident review and corrective action processes

These measures support compliance with UK GDPR Articles 33 and 34 (Breach Notification) and Article 32(1)(d).

4.4 Data Protection by Design and Default
(ISO/IEC 27001 Annex A.8.11 – Data Masking; A.8.24 – Use of Cryptography; A.5.12 – Classification of Information)

Technical and organisational safeguards are embedded into system design to minimise data protection risks.

Controls include:

- Application of pseudonymisation where appropriate
- Data minimisation practices
- Logical data segregation
- Role-based access controls
- Encryption of data at rest where required
- Privacy considerations in system architecture decisions

These measures ensure compliance with UK GDPR Article 25 and reinforce security obligations under Article 32.

4.5 Supplier & Sub-Processor Controls
(ISO/IEC 27001 Annex A.5.19–A.5.22 – Supplier Relationships and ICT Supply Chain Security)

Third-party processing is subject to structured governance and oversight.
Controls include:

- Clear and unambiguous contractual arrangements
- Due diligence in the selection of sub-processors
- Security review of supplier controls
- Ongoing monitoring of supplier performance where applicable

These controls ensure compliance with UK GDPR Article 28(1)–(4) and the Data Protection Act 2018 processor obligations.

ISO27001, UK GDPR / DPA Mapping

Scope: Technical & Organisational Measures (TOMs)

TOMs Section	Control Theme	ISO/IEC 27001:2022 Annex A Controls (with reference to ISO/IEC 27002:2022 guidance)	UK GDPR / DPA References

1.1 Hosting Environment & Infrastructure Security	Cloud hosting & supplier security	A.5.19 Supplier relationships;
		A.5.20 Supplier agreements;
		A.5.21 ICT supply chain security;
		A.5.23 Information security for use of cloud services
			UK GDPR Art. 28(1)–(3);
			UK GDPR Art. 32(1);
			DPA 2018 (Security of processing)

1.2 Physical Access Control	Physical security	A.7.1 Physical security perimeters;
		A.7.2 Physical entry controls;
		A.7.3 Securing offices, rooms and facilities
			UK GDPR Art. 32(1)(b);
			UK GDPR Art. 5(1)(f)

1.3 Electronic Access Control	Logical access control	A.5.15 Access control;
		A.5.16 Identity management;
		A.5.17 Authentication information;
		A.8.5 Secure authentication
			UK GDPR Art. 32(1)(b);
			UK GDPR Art. 5(1)(f)

1.4 Internal Access Control (RBAC + MFA)	Access rights & authentication	A.5.15 Access control;
		A.5.18 Access rights;
		A.8.2 Privileged access rights;
		A.8.5 Secure authentication
			UK GDPR Art. 32(1)(b);
			UK GDPR Art. 28(3)(c)

1.5 Isolation & Segregation of Data	Segregation of systems and networks	A.8.20 Network security; A.8.21 Security of network services; A.8.22 Segregation of networks	UK GDPR Art. 25; UK GDPR Art. 32(1)(b)

1.6 Pseudonymisation & Anonymisation	Data masking & cryptography	A.8.11 Data masking;
		A.8.24 Use of cryptography;
		A.5.12 Classification of information;
		A.8.10 Information deletion
			UK GDPR Art. 25;
			UK GDPR Art. 32(1)(a);
			UK GDPR Art. 5(1)(c)

2.1 Data Transfer Control (TLS 1.2+)	Encryption in transit	A.8.20 Network security; A.8.21 Security of network services; A.8.24 Use of cryptography	UK GDPR Art. 32(1)(a); UK GDPR Art. 5(1)(f)

2.2 Data Entry & Change Control (Logging + Change Mgmt)	Logging & change management	A.8.15 Logging;
		A.8.16 Monitoring activities;
		A.8.32 Change management;
		A.5.37 Documented operating procedures
			UK GDPR Art. 5(2);
			UK GDPR Art. 32(1)(d)

2.3 Data Integrity Monitoring (CrowdStrike + FIM)	Monitoring & integrity	A.8.7 Protection against malware;
		A.8.8 Management of technical vulnerabilities;
		A.8.15 Logging;
		A.8.16 Monitoring activities
			UK GDPR Art. 32(1)(b);
			UK GDPR Art. 5(1)(f)

3.1 Availability Control (Backups, UPS, AV, Contingency)	Backup & operational resilience	A.8.13 Information backup;
		A.7.11 Supporting utilities;
		A.8.7 Protection against malware;
		A.5.29 Information security during disruption
			UK GDPR Art. 32(1)(b);
			UK GDPR Art. 32(1)(c)

3.2 Disaster Recovery & Timely Restoration	Business continuity recovery	A.5.30 ICT readiness for business continuity; A.8.14 Redundancy of information processing facilities	UK GDPR Art. 32(1)(c)
3.3 Architectural Resilience & System Hardening	Vulnerability and resilience	A.8.8 Management of technical vulnerabilities; A.8.9 Configuration management; A.8.14 Redundancy	UK GDPR Art. 32(1)(b); UK GDPR Art. 32(1)(d)
4.1 Security Awareness & Training	People controls	A.6.3 Information security awareness, education and training	UK GDPR Art. 32(4); UK GDPR Art. 5(1)(f)

4.2 DPIAs & Risk Management	Risk & privacy governance	A.5.4 Management responsibilities;
		A.5.7 Threat intelligence;
		A.5.36 Compliance with policies, rules and standards
			UK GDPR Art. 35;
			UK GDPR Art. 25;
			UK GDPR Art. 32

4.3 Incident Response Management	Incident handling	A.5.24 Incident planning and preparation;
		A.5.25 Assessment and decision;
		A.5.26 Response;
		A.5.27 Learning from incidents
			UK GDPR Art. 33;
			UK GDPR Art. 34;
			UK GDPR Art. 32(1)(d)

4.4 Data Protection by Design and Default	Privacy engineering	A.8.11 Data masking;
		A.8.24 Use of cryptography;
		A.5.12 Classification of information;
		A.5.15 Access control
			UK GDPR Art. 25;
			UK GDPR Art. 32

4.5 Supplier & Sub-Processor Controls	Third-party governance	A.5.19 Supplier relationships;
		A.5.20 Supplier agreements;
		A.5.21 ICT supply chain security;
		A.5.22 Monitoring supplier services
			UK GDPR Art. 28(1)–(4); DPA 2018 (Processor obligations)