



Cyber Security Summary Statement



The copyright of this document is vested in Kao Data. This document may only be reproduced in whole or in part, or stored in a retrieval system, or transmitted in any form, or by any means electronic, mechanical, photocopying or otherwise, with the prior permission of Kao Data

Located on SharePoint: IMS: Procedures

Controlled Document: 000

Kao Data Campus Locations

- London Road, Harlow, CM17 9NA
- Galvin Road, Slough, SL1 4AN
- Rowdell Road, Northolt, UB5 6AG

Document Change History

Version No.	Date Issued	Update Details	Issued by	Approved by
V1.0	18/01/2021	Original Draft Document	Graham Webber	Jashan Babra
V1.1	14/06/2022	Revised – updated version – current reflection	Gary Kilmister	N/A
V2.0	15/06/2022	Published Version	Gary Kilmister	Gary Kilmister
V2.1	25/06/2023	Annual review - Reviewed and updates made	Gary Kilmister	Gary Kilmister
V2.2	10/07/2023	Minor amendment made to footer to remove reference to ISO standards	Katie Harper	Gary Kilmister
V2.3	27/07/2023	Final version submitted for Sign off and publish	Gary Kilmister	Paul Finch Lee Myall
V3.0	28/07/2023	Published Version	Gary Kilmister	Gary Kilmister

Distribution List

Copy Number	Job Title / Purpose	Location
000	Master	SharePoint

Cyber Security Summary Statement



1. Introduction

Launched in 2018, Kao Data develop and operate advanced data centres for high performance computing. From our hyperscale inspired campus in the heart of the UK's Innovation Corridor between London and Cambridge and our facilities in Slough and Northolt, we provide HPC, cloud, AI, and enterprise customers with a world-class home for their compute.

2. Summary Statement

KAO Data was awarded the Cyber Essentials PLUS certification originally in December 2020. Latest re-certification was completed in December 2022. This certification requires us to ensure a number of standards are met with regards to cyber security. This includes a hands-on technical verification to ensure the standards are implemented.

<https://www.ncsc.gov.uk/cyberessentials/overview>

<https://iasme.co.uk/cyber-essentials/>

KAO Data is also certified to ISO27001 which establishes, implements, maintains, and continually improves an information security management system.

Each Laptop or computer device has 2 different Anti-Virus/malware Engines:

- Webroot Secure Anywhere Anti-Virus
- Fortify for Endpoint, powered the Sentinel One agent.
 - The Fortify for Endpoint is monitored by a 24/7 Security Operations Centre, that can quarantine the device if the event of suspicious activity while remediation work is completed.

A Microsoft Windows Active Directory Domain controller is in operation at KAO Data (Harlow Campus) to implement security policies on the users and devices, including password policies and device restrictions. No data exists on this network (it is contained in Office 365), so we have not implemented MFA to gain access to this network.

Multi-Factor authentication is in place for accessing the Office 365 portal for emails and file data, as well as accessing any other resources on Office 365, in particular outside local network, with the added security of Number Matching now deployed.

We review system access on regular intervals to ensure the user access lists and rights are current. (IT Platform Matrix)

Internet access from the KAO Data corporate and guest networks are controlled by a ZyXel USG Firewall that utilises active IDP and ADP (Intrusion Detection and Prevention and Anomaly Detection and Prevention) signatures that is actively scanning traffic for known attacks and blocking them. The device also has a Content Filtering Engine and its own Anti-Virus signatures.

We currently have an external email filtering solution that will filter spam as well as malicious phishing email attempts. This also includes a URL scanning technology that will scan a URL when clicked, not just at the point of delivery.

Patches are deployed automatically from the Remote Monitoring and Management software and IT are alerted to any devices that are out of compliance with security patches.

Document Title:	Cyber Security Summary Statement	THIS DOCUMENT IS UNCONTROLLED IN HARD COPY FORMAT	Review Date:	28/07/2023
Version Number:	V3		Classification:	Internal
Document Owner:	Compliance		Page No.	Page 3 of 4

Cyber Security Summary Statement



Regular security awareness training courses and fake phishing emails are delivered to staff to identify any security training that is needed.


Regular encrypted backups of the Office 365 data, including Email and SharePoint, are stored in a secure storage location. These backups are triggered at least 3 times per day. A system state backup of the domain controller is also taken daily.

We have internal policies and procedures that support the above either via the ISO27001 or Cyber Essentials Plus.

- Access Control
- Backup Policy
- Computer and Mobile Device
- Cryptography
- Email and Internet Use
- Network Security
- Passwords
- Physical Security
- Teleworking Policy
- Logging & Monitoring
- Patch Management

3. Sign off

Signed

DocuSigned by:

 A8EE0FF33B86457...

Lee Myall

Chief Executive Officer, Kao Data
 Published: July 2023

Signed

DocuSigned by:

 F3849356F76B49B...

Paul Finch

Chief Operating Officer, Kao Data
 Published: July 2023

Document Title:	Cyber Security Summary Statement	THIS DOCUMENT IS UNCONTROLLED IN HARD COPY FORMAT	Review Date:	28/07/2023
Version Number:	V3		Classification:	Internal
Document Owner:	Compliance		Page No.	Page 4 of 4