KAO DATA

Physical Security Policy

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
V2.0	10/05/2021	Original Document	Jashan Bahra	Paul Finch
V2.1	30/05/2022	Draft revision, new format, and updates	Gary Kilmister	Paul Finch
V3.0	01/06/2022	Published version (signed off)	Gary Kilmister	N/A
V3.1	25.01.2023	Review & update of format	Niki Greene	Gary Kilmister
V3.2	27/06/2023	Revisited Document and re-publishing, updates made regarding location specifics	Gary Kilmister	Gary Kilmister
V3.3	10/07/2023	Minor amendment made to footer to remove reference to ISO standards	Katie Harper	Gary Kilmister
V3.4	27/07/2023	Sign off and Publication of Document	Gary Kilmister	Paul Finch Lee Myall
V4.0	28/07/2023	Published version (signed off)	Gary Kilmister	Gary Kilmister

Distribution List

Copy Number	Job Title / Purpose	Location
000	Master	SharePoint
001	Site Copy – Displayed	Harlow Breakout Room
002	Site Copy – Displayed	Slough Staff Office
003	Site Copy – Displayed	Northolt Staff Office

Contents

Contents

1. Introduction 4
2. Purpose 4
3. Designing Secure Area Guidelines 4
3.1 Principles of Secure Areas 4
3.1.1 Physical Security Perimeter 4
3.1.2 Physical Entry Controls 5
3.1.3 Securing Offices, Rooms and Facilities 5
3.1.4 Protecting Against External and Environmental Threats 5
3.1.5 Public Access, Delivery and Loading Areas 5
4. Working in Secure Areas 6
4.1 Do: 6
4.2 Don't: 6
5 Sign Off: 6

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. Purpose

KAO Data has designed this Physical Security Policy to provide guidelines to reduce the potential risks involved with the physical aspects of security.

The purpose of this document is to give clear guidance to employees, contractors, third parties and other individuals on what is expected of them whilst accessing or working within a physical area that has been designated as secure.

Secure areas are necessary to protect the physical and information assets of the company and its customers from a loss of confidentiality, integrity, or availability, but such areas only remain secure if the people accessing them follow the appropriate protocols. This document gives the reader an indication of the thought and preparation that has been invested in creating a secure site and secure areas within the site, and details how to ensure that these remain secure whilst not obstructing the business carried out within.

These guidelines apply to all secure areas in use within the organisation; further detailed procedures will be made available for specific facilities should you be required to access them.

3. Designing Secure Area Guidelines

3.1 Principles of Secure Areas

The design of secure areas is a complex business that requires that the designer undertake a full and comprehensive assessment of the risks associated with each specific facility, second-guessing the most likely methods of unauthorised access, and addressing them one by one.

However, as with all security design, the measures put in place must remain appropriate so that the users of the facility are not unreasonably hampered by them and are able to carry out the task for which the facility was created.

In line with the ISO 27001 information security standard there are several points that have been addressed when designing the secure areas and these have been understood by the user so that they are not inadvertently compromised.

3.1.1 Physical Security Perimeter

The first consideration is to define the location and perimeter of the secure area. In general, secure areas are sited to avoid access or visibility to the public or unauthorised people and measures are taken to avoid drawing attention to them.

A 3M high fence that incorporates anti-ram sensors interfaced with the other security & CCTV systems encompasses each Kao Data Campus.

All entry points around the physical security perimeter will be risk assessed including perimeter fencing, gates, doors, windows, access hatches, lift shafts, ceilings, and walls. Intruder alarms and Closed-Circuit Television (CCTV) may be installed to protect entry points and warn of security breaches.

The Datacentre has closed-circuit monitoring (CCTV), video surveillance as needed, both internally and externally, with all video footage and kept for a minimum of 90 days for the purposes of meeting security best practices and various regulatory requirements such as PCI DSS at Harlow, but Slough and Northolt currently have a minimum of 30 Days (PCI-DSS approved).

3.1.2 Physical Entry Controls

All approved entry points to the secure area will be protected. Doors will typically have a form of two-factor authentication such as a swipe or proximity card and a personal identification number (PIN) or Biometric scan at our Harlow facility. For Slough and Northolt, Kao Data demise works on Swipe for secure areas and use of iTRAC (Tracker) Key cabinets, where authorisation to keys are set on approval level (Users who have access to key box can only remove keys they are approved for). iTRAC boxes are linked to access control cards and have configuration set to which keys user is authorised to).

Authorisation to the secure area will be granted using a strict procedure with access rights reviewed on a regular basis to check that everyone that has access is approved.

All users of secure areas (including visitors) will be required to wear a visible and current ID badge.

Third party visitor access to the secure area will usually need to be requested in advance and such visitors must be signed in at reception and always supervised by an authorised member of staff.

3.1.3 Securing Offices, Rooms and Facilities

Individual rooms within the secure area may also be protected by additional security. Such rooms will typically include server rooms, communications rooms, Human Resources, directors' offices, Meet-Me rooms and plant rooms (such as power and air conditioning).

Depending on the type of facility, users of such individual rooms may need to have specific access and be required to sign in and out. In some cases, mobile phones, cameras or other video or audio recording equipment will not be allowed.

Meet-Me rooms are highly secure and require three level authentications, card, pin and biometric at our Harlow facility, but on secure authorised key at our Slough and Northolt facilities.

Vacant areas within the secure perimeter will be locked and regularly checked for signs of unauthorised entry or use.

3.1.4 Protecting Against External and Environmental Threats

In addition to being covered by the organisation's business continuity plans, secure areas may require further consideration to ensure that any external events such as fire, flood or earthquake will not expose the confidentiality, integrity or availability of the contents.

This may affect the siting of secure locations and the procedures used for reacting to events such as fires, subject to health and safety considerations.

Siting and protection of equipment, supporting utilities and cabling should also be considered and regular maintenance scheduled.

3.1.5 Public Access, Delivery and Loading Areas

Where a secure area includes the need to provide access to the public and /or to accept deliveries this should be segregated as far as possible with a controlled interface within the secure perimeter.

A separate delivery or holding area should be used so that deliveries may be inspected prior to them being accepted into the secure area. Such inspection should happen as soon as possible after the delivery and be comprehensive enough to assess the likelihood of any threats being present.

.

4. Working in Secure Areas

For all employees, third parties and other stakeholders who are given access to a secure area the following will apply.

4.1 Do:

- ✓ Ensure you understand the specific instructions for all secure areas to which you are granted access.
- ✓ Challenge and/or report anyone not wearing an ID.
- ✓ Remain vigilant whilst within the secure area.
- ✓ Always escort your visitors.
- ✓ Inspect all deliveries as soon as possible.
- ✓ Check that doors are secure before leaving if you are the last one out of the secure area.
- ✓ Inform security of visitors that you are expecting.
- ✓ Check vacant areas for signs of unauthorised access.

4.2 Don't:

- × Tell anyone about the secure area if you are requested not to
- × Allow anyone to tail-gate behind you through a secure entry point.
- × Keep secure doors open for longer than necessary.
- × Allow anyone to work in the secure area on their own unless by prior arrangement.
- × Lend anyone your ID card.
- × Expose your ID card to possible theft or loss.
- × Tell anyone your PIN code.
- × Write your PIN code down.
- × Use any photographic, video or audio recording equipment within the secure area unless by arrangement with security
- × Leave classified information unattended in clear view.
- × Take food and/or drinks into secure areas

By following these simple rules, the security of the organisation's information assets may be protected effectively with minimum disruption to everyday work.

5 Sign Off:

Signed

DocuSigned by:

A8EE0FF33B86457...

Lee Myall
Chief Executive Officer, Kao Data
Published: July 2023

Signed

DocuSigned by:

Paul Finch

F3849356F76B49B...

Paul Finch
Chief Operating Officer, Kao Data
Published: July 2023